Homeland Security

Department of Homeland Security
Data Privacy and Integrity Advisory Committee

OFFICIAL MEETING MINUTES

Tuesday, December 6, 2005
J. W. Marriott Hotel
Capitol Ballroom (E&F)
1331 Pennsylvania Avenue NW
Washington, DC 20004

MORNING SESSION

Ms. Richards: Good morning. My name is Becky Richards. I'm the Executive Director of the DHS Data, Privacy and Integrity Committee. We're bringing this meeting to order. Lisa, it's all yours.

Ms. Sotto: Thank you very much. Thank you for joining us this morning. As the first order of business, I would like to thank Paul Rosenzweig deeply from the bottom of my heart. Paul recently stepped down as Chairman of this committee to take a position with DHS. I want to express the committee's appreciation and my deep gratitude for Paul's incredible stewardship from the inception of this committee. Paul has left us with a meticulous blue print to follow. Thank you, Paul.

To the more mundane, if you are interested in signing up for public comments, the sign up sheet is right outside the door. Please do sign up. We cannot take your comments if you don't sign up in advance. Please turn off your cell phones if you have them on. This is a good time to do it, and I will do the same. If you need written materials, they're outside the door if you have not picked them up on the way in. Now, turning to our first speaker this morning -- I am sorry to announce that the secretary, who was planning to join us this morning, has instead been called to the White House. We have an excellent replacement in Paul Rosenzweig, who is now sitting on the other side of the table, ready to be peppered with questions, I think, from this committee. Paul has recently started as a counselor to the DHS Undersecretary Policy Directorate. Paul is a former Fellow at the Heritage Foundation and was an adjunct professor of law at George Mason University. Thank you, Paul.

REMARKS ON DEPARTMENT OF HOMELAND SECURITY

Mr. PAUL ROSENZWEIG

Mr. Rosenzweig: Thank you, Lisa, and thank you for those kind words. It is, I think, a bit surreal to be over on the other side of this table from you all, but it is also a very, very great honor. Let me first express Secretary Chertoff's apologies, but it was at about 3:00 o'clock last -- yesterday afternoon or 2:00 o'clock that he was asked to come to the White House for a briefing this morning. So he's three blocks away, and I know that he actually probably would prefer to have been here. But -- well probably not. But I was asked to come and speak in his stead. I have his talking points, so the precise words will be mine, but the thoughts, I assure you, are the ones that the Secretary would have conveyed to you were he here today to speak with you. I first want to, on behalf of the Secretary, acknowledge and thank you all for your hard work. I want to thank Lisa, the acting chair, for her leadership on the committee. I would also like to, on behalf of the Secretary, thank the Acting Chief Privacy Officer, Maureen Cooney, and the Privacy Office for all the hard work it does, and I want to, particularly, on behalf of the Secretary, express this thanks to you, the committee members, for your hard work and advice as the department continues to integrate privacy measures into our programs and address privacy concerns.

In particular, the Secretary asked me to tell you that he appreciated, very much, your recommendations on using commercial data to reduce false positives, a report that he has received and has reviewed. And also, to thank you for what, he anticipates, will be your work on Secure Flight, other screening initiatives, as he understands the forthcoming work of this committee. I also know that you've conducted several site visits to DHS facilities, including the National Targeting Center, to get a first-hand view of how our components work, and I join the Secretary in thinking that that is an absolutely vital aspect of what you do to get a handle on how the working components of the department operate. In each of the areas that you've been examining, I want to stress the importance of privacy and its protections. We can't achieve security without appropriate privacy protections. We don't want security at any price. We want security that is consistent with our freedoms and values and with the movement of people and commerce across our borders.

We cannot respond to terror by getting into a shell. We can't respond to terror by cutting off all commerce with foreign nations. But, in order to effectively manage risk, we must have, on the other side, information. Information about the terrorist threat vectors, information about shippers, information about travelers, and we must use technology to allow us to determine whether a particular individual or a shipment represents a threat. As we use that information and develop systems to achieve more effective risk assessments and risk management and thus, hopefully, more effective security. There are several core privacy principles that really ought to guide the department's efforts, and the core privacy principles that will be guiding the department as we go forward are, first, we need to make sure that privacy protections are integrated into the full spectrum of our security programs at all stages of development. Not just as an afterthought. And that is something I can wholeheartedly agree with because that is, I think, the vital aspect of how we're going to embed privacy principles into new operating systems. We also need to have clear guidelines and protocols on how personal information is collected, used, stored, shared, and ultimately, destroyed. In each of our programs, those guidelines may differ depending upon the uses and the nature of the data that is being collected, but each and every program should strive to have guidelines of that form. Third, the process has to be transparent and with robust safeguards. We want to maintain the public's trust and confidence in our programs, both at home and with our international partners.

And we can only do that if, to the maximum extent practicable, the programs are transparent to outside view. Now they can't be completely transparent because, as you surely know, full transparency will, in some instances, frustrate the security that is at the bottom of the program itself but to the extent that it can be done. So, a core principle ought to be transparency. We need to tailor the information that we collect to achieve maximum benefit and use with minimum intrusiveness. That is a hard challenge. It's very easy to say, but that is the goal. And finally, as a core principle, we need to have an effective redress mechanism with every one of our programs so that individuals can insure the accuracy of their personal information. That, too, is easier said than done, but it is one of the principles that guide the department. Now, there are three areas where we have to continue to apply these principles as we develop departmental programs. The development and use of new or existing technologies, managing risk through data analysis, and maintaining international partnerships, and I want to speak to each of those three briefly. With respect to integrating privacy protections into technology, as we increase our use and reliance on new technology, whether it's at airports, seaports, along our borders, privacy protections will need to be woven into the fabric of those programs at their inception.

The DHS Privacy Office plays a key vital role in that process to make sure that appropriate protocols are in place and to conduct the necessary privacy assessments. The moment of the piece or our collection of data can be used to identify an individual, there's a potential privacy issue. And DHS will have to begin its privacy assessments at that point. If no personal information is used, however, we'll note that as well. If personal information is used in some manner, we will need to engage in the full privacy impact analysis process. Regarding the use of data analysis, an area that I know has been of concern to the committee and to the public at large. Though it is of concern, it is, in some sense, absolutely vital and the core of what we do. The sheer magnitude of people and cargo entering our country everyday requires us to use some form of technology and analysis to identify potential threats in large collections of people, cargo, and data. This year alone, for example, Customs and Border Patrol Inspectors processed 86 million air passengers arriving from overseas. That's exclusive of domestic travel, 86 million. That's a new record, and that exceeds pre 9/11 travel volume for the first time since 2001.

We can't inspect each of those 86 million people rigorously and completely. We need to explore how analysis of large sets of data and information may be helpful in identifying possible terrorists and terrorist activity and focusing our resources on those who present a higher risk profile. But, it's also vital that we understand the full impact of the technology and the new knowledge and information that that technology develops -- that that technology generates rather. As we engage technology to extend our reach, we also need to expand our appreciation and protection of privacy. The examination of large fields of data raises clear privacy concerns. The Secretary is convinced it's an absolutely vital aspect of targeting scarce resources, but it's one that must be done with sensitivity to the existence of potential privacy implications.

Hopefully, if we do our jobs right and build the privacy protections in at the beginning of the system's development, we can mitigate the privacy risk and maximize the security benefits. The final piece of what we are doing, an area where these principles will have application is in the area of international cooperation. A subject I know you're going to be hearing about a little later today. We know now, for sure, that privacy doesn't end at the water's edge. It used to be said that partisanship ended at the water's edge. Now we know that privacy does not. If we want to protect the privacy of our own citizens, we are going to have to be willing to protect the privacy of our international partners and their citizens. And that means we have to protect shared information and continue to demonstrate a level of trust that is, as I'm sure you will hear, an ongoing process. But, we've had some successes of which the department is, I think, justifiably proud. For example, in September, the first ever joint review with the EU was conducted regarding CBP's collection of PNR, passenger name record data from European travelers. The feedback from the EU is that the review was fully successful. I wouldn't want to prejudge the final reports, but every indication we have is that through a series of negotiations and discussions, we've managed to accomplish all of our security needs in ways that satisfy our international partners, that we are trustworthy possessors of data. I should note, as an aside, that many in Europe are moving forward with PNR collection programs themselves in the near future, and I trust that the Privacy Office will be equally vigorous in insuring that American data is protected in the EU to the same or a higher degree. Moving forward then, we're going to have to uphold our commitment to our international partners while respecting the legal and cultural differences that often govern very different responses. In conclusion, the committee here will continue to play a critical role in helping us achieve our security mission consistent with data privacy and integrity mandates. On behalf of the Secretary, I want to express his view that he looks forward, very much, to hearing from you in the future and that he appreciates your ongoing partnership, recommendations, and support for our efforts and for those of the Acting Chief Privacy Officer and the Privacy Office. What you do is absolutely vital and is of great assistance. I can attest on a personal level now, that he reads the reports that you send up, which is worthwhile. So, on that note, I'd like to thank you very much for your attention. Again, apologize for the fact that I'm not Secretary Chertoff, and perhaps, if possible, answer a few questions.

Ms. Sotto: Thank you very much, Paul. That was very helpful. As with prior custom, if you have questions, please turn your name cards up. I will use the chair's prerogative and ask the first question.

Paul, your office is in charge of setting policy at DHS. The Privacy Office also sets policy. How do you see the two offices meshing?

Mr. Rosenzweig: Well that's a great question. I think at least the first cut answer is, it hasn't been fully built out yet. The office that I work in was created on October 19th. So, final interaction processes are still being developed. That having been said, I think it is fair to say that I anticipate that the Policy Office will work exceedingly closely with the Privacy Office. Many of the policies that we are developing have, embedded within them, privacy concerns and ought to have, embedded within them, privacy concerns, and I cannot see us addressing them without engaging the Privacy Office fully as to the extent of the privacy impacts that are a subset. To give you but one example, our office has been and will continue to be engaged in the development of policy relating to the architecture of Secure Flight. Which we anticipate will be rolled out in the near future. We can't do that without asking the privacy questions that go with Secure Flight. We can't ask those questions without talking to the Chief Privacy Officer. I would note that, at least as an initial matter, Maureen, the Acting Chief Privacy Officer, has been in regular attendance at her ongoing policy meetings that occur once or twice a week where all the policy leaders kind of get together. And I anticipate that other types of mechanisms, both formal and informal, will be developed that will allow us to fully take advantage of the expertise and information in the Privacy Office. And make sure that their concerns and interests are fully developed as a part of the ongoing development of any program or policy that has privacy impacts.

Ms. Sotto: Thank you very much. Michael Turner.

Mr. Turner: Paul, I apologize for coming in late and missing the first half of your presentation. In fact, that the Secretary couldn't be here provides a great opportunity for you to visit with your former committee. So, I'm glad that you're here today. You made an interesting remark to the extent that you were highlighting the recognition of legal and cultural differences that govern very different responses when considering privacy policies. And as a follow on to the EU, joint review with CBP, I'm wondering what, if anything, the DHS Policy Office does to systematically account for the legal and, particularly, cultural differences on privacy matters when considering various policy?

Mr. Rosenzweig: We're exceedingly sensitive to the reality that privacy is a highly variable concept, both across international boundaries, between us and the EU for example, and to a lesser degree, but to a very real degree, within the United States. If, by your question, you mean do we take surveys to try and figure out exactly what those differences are? Not yet, but not a bad idea. But what we do do -- do do, in developing all of our responses, is attempt to work closely with our international partners. Particularly, to understand what their concerns are, to advance our own concerns as well on an equal footing. The Policy Directorate that I'm in has, within it, an Office of International Affairs whose sole job is to make sure that the Policy Directorate and above that, the Deputy Secretary and the Secretary have a full understanding of the concerns of our international partners and how they are derived from cultural or legal differences that are relevant to our ongoing discussions.

I can tell you that the Deputy Secretary is in Europe right now. And many of these distinctions are going to be the subject of discussions that they have in the UK and in Brussels as we move forward. As I said, I think we're all pleased that the joint review was such a success. We think that it's actually not a zero sum game, that it's not going to be a trade off between our values and the Europeans. To a large degree, our goal is to make sure that everybody gets what they need out of the agreements and understandings. I'm not willing to believe that that's not possible yet.

Ms. Sotto: Joe Leo?

Mr. Leo: Thank you. Good morning Paul. I was going to ask the Secretary the following question, so do the best you can.

Mr. Rosenzweig: Okay. Sorry I'm not him.

Mr. Leo: The Secretary created the Policy Office in October, and I'm trying to -- my question is to get some insight on the policy direction in the coming year for the Policy Office and with the Department of Homeland Security. I’m going to prompt you to a recent event. One, the 9/11 Commission which handed out some pretty tough language with regard to the job yet to be done.

Mr. Rosenzweig: Uh-huh (affirmative).

Mr. Leo: And, the Secretary -- I'm sorry, the President's recent visit at the borders, talking about securing our borders, et cetera. Could you give us a little bit of insight on the policy direction in the coming year?

Mr. Rosenzweig: Sure. The department is huge. It has 180,000 employees. And before the Policy Directorate was created, you know wags have said that there are 180,000 policy makers. That's a little bit of an exaggeration, but it is absolutely clear that one of the lacks in the originating structure of the department that the Secretary identified in the second stage review was the absence of a coordinating policy shop.

So, at the very first cut, one of the things that the Policy Office is going to be seeking to do is a process oriented managerial kind of piece. Namely, get control of the intra and interagency processes so that we no longer experience, as has sometimes been the case, different parts of the department having divergent views. We're going to try and speak with one voice.

If we get -- once we get the process point out, if you ask me where our focus is, substantively would be, I think you put your finger on at least one of them, both the President and Congress have clearly indicated that immigration will be broadly writ -- you know, including border enforcement, interior enforcement, temporary worker program. All those things will be an item of significant concern to the nation and to the extent that it is so. It will be natural for the Policy Office to have a significant effort in that since DHS owns most of the immigration enforcement and monitoring pieces, and so that will be one of them. For my own part, I would also say that disaster preparedness and response is going to be high on the list as we continue to learn from Hurricane Katrina. There is a robust lessons learned process going on which, we anticipate, will provide us with a whole host of recommendations of better things to do.

And then I think that the third focus, which is probably more in the wheelhouse of this committee and more at the core of what DHS was set up to do, is counter terrorism, protecting the homeland sorts of things. Probably with an emphasis on things like weapons of mass destruction. The Secretary has said, clearly, that we want to target our resources at the more catastrophic risks to the extent that we can, and that that is a better use of resources and so, to effectuate that, a large policy focus will be on radiation, nuclear biothreats and new programs to impede those threats and insure that they don't come to the homeland.

Ms. Sotto: Let's see. Kirk Herath?

Mr. Herath: Thank you. Paul, as our former chairman, and as you know, as we're starting to get our processes together here, now that you're on the inside in the policy making position, do you have any suggestions or recommendations about how we might focus our limited time and resources on work products or output that would be most relevant and helpful to you and DHS?

Mr. Rosenzweig: That's a great question. I'm going to want to mull that for a little bit. I know that the Deputy, in his first meeting, asked you to focus on screening programs because that is, broadly speaking, where the data privacy and integrity questions -- you know, that rubber meets the road of security. To that extent, I know that the Secretary and the Deputy Secretary remain very interested in hearing your concrete recommendations about Secure Flight, for example. If I would broaden it a little bit, I would say that -- well, when I was in your -- over on the other side, my focus was very much, on individuals and individual data because that seems to be where a lot of the public concern is. But a large fraction of the screening that we do is not at the individual traveler level but at the cargo level, at the shipment level, and I think that there's a lot of work that can profitably be done and recommendations that would be very much welcome in the design of new cargo tracking, cargo screening functions. It may not have the same public resonance because it generally doesn't seem to have the same -- generate the same level of public concern. But, that would be a very profitable one as well. But I'm going to think about that, Kirk, and if I think of any others, I'll call Lisa.

Ms. Sotto: Yeah, I would specifically ask you to think about that. You're in a better place than most people.

Mr. Rosenzweig: Yeah. It's a great question. I just don't know the answer.

Ms. Sotto: We'll hold you to it. Charles Palmer?

Mr. Palmer: Paul, in the Emerging Technology and Application Subcommittee discussions with the S&T Directorate, we kind of got the impression that very talented, very deeply skilled people doing a whole lot of work. But, not necessarily thinking about policy level direction on the application of new technology. Is this something that your office will be doing on things like -- your setting policy for the reasonable use or application of things like RFID and biometrics and so on?

Mr. Rosenzweig: Yes. I mean -- as I said, we're new, and we've identified a whole host of areas where we can do more in the policy realm, and one of those is S&T, RFIDs. Again, many of the technologies have privacy implications. So, I imagine we would be fully engaged with the Privacy Office in defining the scope and reasonableness of using RFID technology, and that too, is clearly an area -- I mean, that fits into the cargo area that I was just sort of talking about with Kirk, where the recommendations of this committee would be ahead of the process development curve to a great degree and would be able to carry -- you know, certainly, a great deal of weight with me, and certainly be influential within the department.

One of our tasks in the Policy Office more broadly written is -- you know, I said earlier, there were 1800 employees. There are only a hundred in the policy shop as initially constituted. And so we're going to have to develop our connections to the various components of DHS, both up at the headquarters level like S&T and state and local grants, and also in the active component levels like, you know CBP, ICE, TSA. And, as you might have mentioned, that's an organic process. It doesn't happen overnight by fiat. It has to develop kind of, as in all human endeavors, by bits and pieces over time. If you have my boss, Stewart back in the year, I'm sure he will be able to actually tell you -- well, I hope he'll be able to tell you he's made a great deal of progress in that.

Ms. Sotto: Thank you. I'm going to, unfortunately, need to cut questions a little bit short unless, Maureen, you're willing to cede a little bit of time?

Ms. Cooney: Sure.

Ms. Sotto: All right. We'll do another five minutes, all right? John Sabo?

Mr. Sabo: Thanks you, Paul. I've already welcomed you, so I won't have to go through that again. You talked about trust, and in the examination we did of Secure Flight, we have a draft that will be acted on by the committee. One thing we discovered was, in complex systems like Secure Flight and many others in the department, you have interaction from one system or one program with other programs and other systems. They're all networked, and you're dealing with multiple policy points. You might be dealing with airline systems, and all of that must be harmonized to some degree, and I guess, as a practical question, I'm wondering if you've given any thought or have views about how you can reach out to these multiple policy stakeholders, as well as the people in those organizations who use these systems and do two things. One would be to make sure the policies are harmonized, and make sure that there are -- you know, that actually the activities associated with the networks are enforced according to the policies. Otherwise, the department can be labeled or -- you know, criticized for having an untrusted system or for deviating from policies. When, in fact, it's a subordinate system or an external entity outside the government. So, I don't know if you have thoughts about that or if not thoughts now, if that's something you can look into?

Mr. Rosenzweig: Well, actually, I do have some thoughts about it, though I hadn't thought about it in terms of the external systems. But, with respect to intra department systems within DHS, and to a lesser degree but to a real degree interdepartmental systems, I think our view, in the Policy Directorate, is that that's the whole purpose for what we are doing - is to insure consistency across a range of operational components in policy.

One of the areas where I can already see that being effectuated is in the development of the information sharing environment which was required by Congress under IRTOA, the Intelligence Reform and Terrorist Protection Act of 2004. The program manager for that resides in the office of the Director of National Intelligence, John Rusack. He has an interagency process ongoing for information sharing that engages the intelligence community, the law enforcement community, state -- you know, you have DHS.

DHS is taking the lead on developing the pieces that relate to coordination with state and local stakeholders who are our main customers in the information sharing environment, construct our main customers are not the DNI. We're a customer of his really. And in that context, we're leading, from the Policy Office, an effort to coordinate all of the -- an understanding first, a survey of all of the things that all of the different components do with state and local people.

Once we get a handle on the survey, we can get to the complex question of how we share information with state and locals that is derived from classified information, but it itself has to be unclassified so it can actionable. It's a difficult process, but the Policy Office, in this instance, has already been designated to serve as a focal point both out to the IS -- Information Sharing Council and down to our components. I would anticipate that as we get our legs under us, get the staff to do it, and get ourselves a better sense of all of the different places in the department where that type of thing needs to be done, that we'll slowly but surely take on more roles like that. Again, it is an organic process. We haven't ◎ you know, October 19th, we didn't just start making everybody report to Stewart.

Ms. Sotto: All right. I think I'm going to need to cut off questioning. I'm sorry. We can, of course, call Paul. And I'm sure you work. Thank you so very much Paul.

Mr. Rosenzweig: Thanks for having me.

Ms. Sotto: We appreciate your participation.

Mr. Rosenzweig: I want to just want to close by expressing my own personal appreciation for the work you're doing and the effort. Having sat over there, I know that it's an awful lot to ask for from a bunch of people who don't get paid and if only the honor of -- you know, serving, but I want to assure you that what you're doing is very much worthwhile and of very great interest to me, to the Undersecretary for Policy, to the Privacy Office, to the Deputy and to the Secretary. So, I would urge you to continue and to help us find the right answers to a very difficult set of questions. Thanks a lot.

Ms. Sotto: Thank you for joining us. Our next speaker is Maureen Cooney. Maureen is the Acting Chief Privacy Officer of the Department of Homeland Security. In that role, Ms. Cooney is responsible for privacy compliance across the department, which includes assuring that the technology used by the department to protect the U.S., sustain privacy protections related to the use, collection and disclosure of personal and department information. Ms. Cooney, previously, was Chief of Staff for the Privacy Office, assisting the Privacy Officer in developing and representing the DHS Privacy Office policies, programs and goals.

Before joining the Privacy Office in January of 2004, Ms. Cooney worked on international privacy and security issues as legal advisor for International Consumer Protection at the U.S. Federal Trade Commission. Thank you.

PRIVACY OFFICE UPDATE

Ms. MAUREEN COONEY

Ms. Cooney: Thank you, Lisa. And thank you to all the members of the committee. I want to echo, as robustly as I can our support and thanks to this committee for your support and interest in the privacy issues at the Department of Homeland Security. They, of course, are the main focus of the work in the Privacy Office, but they are of great concern to the American people and for your service, I thank you on behalf of the department. It is a privilege to serve as the Acting Chief Privacy Officer for the Department of Homeland Security and to report to you today on the activities of the Privacy Office. Since the committee last met in September in Bellingham, Washington the pace of work in the Privacy Office has continued to be very active. I would like to give you a sense, as well as our audience today, of the vitality of the Privacy Office and the issues that we look at. I believe your last meeting was just about two months ago to the date. Notably, the activities that we've been working on during this time include, in our technology group, leadership within the U.S. government on the privacy, legal frameworks and social impacts of biometrics.

Our staff has been working cooperatively, both internally within DHS and across the federal government, in studying those issues and outreaching not only within the United States but, in Europe and other parts of the world. We have taken a leadership role on the development of Real ID, which is a requirement of Congress. We have recently met with members of the public and advocacy groups to learn their concerns and issues as the regulation moves forward on Real ID. We've given counsel within the agency, on information collection and sharing with respect to avian flu and pandemic issues. We've worked extensively with our component FEMA on information sharing that is allowed under the Privacy Act for disaster relief, and public safety, and law enforcement promotion. We have worked extensively as well in giving privacy impact assessment guidance and reviews throughout the agency on all OMB 300 procurements of technology. That was a major undertaking where we looked at more than well over a hundred new systems.

We, furthermore, have given guidance on threshold analysis for technologies within the department, and in the next couple of months, we expect to be reviewing up to 400 systems of the 750 or so systems in the department. So, it's a major undertaking which we're doing in cooperation with other parts of the agency. On the international front, we continue to note that our efforts on international cooperation are most important in building trust and veracity in the way in which we hold and treat information about individuals. Within these past two months, since our last meeting, we have been to Australia, Spain, Germany and Belgium, speaking with our international counterparts. And finally, we've been giving counseling to other components and offices within the department that are strengthening or building privacy offices of their own with which we will be working closely. Those include Immigration and Customs Enforcement and Citizen and Immigration Services among others.

In addition to the daily counseling we provide within the department, we've done some stock taking in these last couple of months. I would like to share with you the goals that I have set for this interim period while I hold the acting position. One of the areas in which we've probably fallen short, just due to staffing and time constraints, is in actually giving written internal guidance. Up to now because it's only been fairly recently that we've had a fuller staff. We have generally been giving one-on-one guidance depending on what the program is or what the proposals were before us. What we're trying to do is to actually put into writing, in a broader way or broader distribution within DHS, internal privacy guidance. While I say that, we've not fallen short in every area, and I would like to note that we have, in particular, taken a leadership role in the federal government in putting out written guidance on privacy impact assessment, how to do them, what questions should be asked and actually training our staff throughout DHS. That is not just privacy staff, that is programmatic staff, people who are looking at and developing security programs. We do hope to finalize date of usage guidance, and to that end, the paper that you distributed to us at the last meeting has been very helpful. We fully endorse the recommendations that you set forth, and that will be the building point for our own internal guidance.

In addition to that guidance, there are other reports that I know Nuala O'Connor Kelly, our Privacy Officer preceding me, mentioned at the last meeting. And we continue to work on moving those forward, our report on the matrix program, on Secure Flight, No Fly which is a required report to Congress, and on data mining, another required report to Congress by the end of this year. All of those are well on their way.

The second major goal that I've set is education and training throughout the department. We've recently been able to fully staff an Education and Training Development Director towards the end of doing a broader type of education, not just for incoming employees, but across DHS. We're planning a privacy awareness week in the first quarter of '06 that will include training on Privacy Act compliance, Freedom of Information Act compliance as the book end to privacy access and disclosure, as well as a workshop on privacy impact assessments and how to do those. We hope that that will be a public workshop similar to the workshop that we held in August on commercial use -- or, I'm sorry, on government use of commercial data in the governments space.

The third major goal that I've set through this interim period is to focus on information sharing and the information sharing environment. To that end, we have been very active already in the interagency process as well as within DHS in looking at protocols that we have or need to set out for information sharing, to counteract terrorism.

While we know we need vibrant information sharing and endorse that, we also need to share information and hold in it an appropriate way.

And finally, the final goal that I have for this interim period is to continue working on international cooperation and ways to bridge our mutual needs for information, to counter terrorism as well as to protect individual privacy. I would like to tell you that we have continued to receive strong support from Congress, and we have been given four federal employee slots to fill in '06. We have filled one of them already with a Senior Advisor, Kenneth Mortensen, who many of you have been working with. We have three more to fill. We have either posted them, or they will be posted. They're in the pipeline for this week, and I want to let you know that we take that as a priority, to fill those slots that Congress has given to us. I thank you very warmly and heartedly for your support and guidance, and I welcome your guidance during my term as Acting Chief Privacy Officer. Thank you.

Ms. Sotto: Thank you very much, Maureen. Questions? Mr. Alhadeff?

Mr. Alhadeff: Thank you, and thank you, Maureen and the Privacy Office, for all the hard work you guys do. I know there's a bunch of late night oil that gets burned over there. I wanted to raise one of the issues that you brought up which was kind of not one of the main topics that you were raising but one of the topics that you spoke about related to avian influenza, and I was wondering two things.

One of them is whether that's an international effort or just a domestic effort? Because unlike Katrina, which is a localized although devastating event, avian flu is a global event where information sharing will be required to actually map how the disease progresses, and have any effective hope of actually containing it before it becomes a pandemic which could be disastrous. And to what extent are there education and training components related to those types of issues? Because they do involve the sharing of personal information, and that is across agencies, not just within agencies.

Ms. Cooney: Thank you, Joe. That's a great question. Well, certainly it is an international effort and from within DHS, we have been viewing it in that way. We know that much of the information that we will need to collect is not only from our own citizens but from visitors coming into the United States. So at this time, really, we're at a planning stage in our discussions with our partners across the globe. On the privacy side, we've certainly given counsel to our Policy Office and to our senior leadership on engagement on the international level and the privacy issues that are attendant to it.

In terms of training, that's an excellent note that you've made, and it is one that I would like to look at more closely in how we should be giving guidance within the department. Informally again, we've worked very closely with Customs and Border Protection, with TSA, and with some others who would be collecting international information. So, more of a one on one counseling situation which is what we have been able to do to date with the staffing that we have. But with respect to a pandemic as well as some other situations, written guidance would be very helpful, and we'll look at that as we plan our training. Thank you.

Mr. Beales: If I could have a brief follow up to that, I noted that CDC has proposed rules on collecting information that is aimed at pandemic concerns. And if you could just address how the departments fit together on that set of issues, I think it would be useful.

Ms. Cooney: We've worked very cooperatively with CDC in terms of information sharing, looking at what types of information sharing, not only DHS but other federal departments. What information we might hold that they might want to draw upon. We have commented on their proposals for collecting information, and in some areas, they have taken our comments, and in other areas, I think they're looking for public input. That's the process to date.

Ms. Sotto: Mr. Barquin.

Mr. Barquin: In most -

Ms. Sotto: Ramon, could you put on your microphone?

Mr. Barquin: Any better? Sorry. Most of what you spoke about, in terms of the active programs of the Privacy Office, really dealt with privacy as you would expect. But, this committee deals with both privacy and data integrity. Data integrity seems to get always left to the back of the bus, because privacy is so much on the front burner. But, I would like to really get a sense from you of what the Privacy Office sees as its responsibility on the data integrity side, and what are you doing for the department in that regard?

Ms. Cooney: I'm sure that as I answer this question, I am going to forget things we're working on, but data integrity is very important to us. I would say beginning, as we look at freedom of information as well as the robustness of the information that we have on hand in our systems. One of the things we look at with every program that exists now and every proposal for a security program is how accurate is the information that we're holding, and if it is not accurate and timely, what is the effect on the individual? So to the extent that we're retaining data and continuing to use data about an individual, we have a real interest, in the Privacy Office, of making sure that that information is robust enough to be relied upon. And for people to be able to get a sense of what information we are using about them in order to seek adequate redress, to update information, to delete information that might not be necessary and to make sure that only the information that is necessary for a program is what is collected and retained. Does that answer part of your question?

Mr. Barquin: That certainly answers part of the question, but at some point, I would appreciate the Privacy Office maybe talking about specific programs about interactions with other parts of the department, and particularly, how does it work visa vi the whole security apparatus of Homeland Security -- I mean data security. What type of information quality initiatives there are and how does the department -- how does the office, the Privacy Office, interact with other parts of Homeland Security?

Ms. Cooney: I'd be happy to follow up on that. I think one other area, that I probably should have emphasized as well, is that when we receive requests from other agencies for information sharing, one of the foremost ways of protecting the integrity of the data that we hold is to make sure that when we're releasing information, it is for a legitimate purpose, necessary for the party receiving it, that they have an adequate basis for asking for the information, and that when we've given notice to individuals, that we're collecting information for a certain purpose, that it isn't then shared for unrelated purposes. And that there is a security protocol with those third parties with whom we're sharing so that the integrity of the data isn't further compromised. But I would be happy to report to you further, and we'll get on that. Thank you.

Ms. Sotto: Thank you. And for the last question, Jim Harper.

Mr. Harper: Thank you, Maureen, for your enthusiasm and your care in your current role as Acting Chief Privacy Officer. You mentioned, in your statement, the Real ID Act and the coming implementation of the regulations under the Act. One of the requirements of the Act is a machine readable feature. And I want to just share with you some thoughts that are my own. I think we may be looking at this in more detail in the committee, and again, these are my own thoughts, and I don't represent any subcommittee in this matter. But, the question of what a machine readable feature is, is an important detail that the DHS and other implementing agencies will be looking at. And I want to emphasize the range of options that are available under that. Frankly, print on paper is a machine readable device at this point, and I think a lot of people are assuming, a lot of people are concerned that rather than the full array of possible devices, the department will gravitate to RFID. And I want to suggest that you look to the experience of the State Department with the E- Passport as, essentially, a lesson in failure at the policy making process. Because the E-Passport, originally, had an RFID chip embedded in it. Meritorious, security and privacy arguments were put forward, and a great deal of effort went into fixing the problems with RFID, and at the end of the day, there was no net benefit from using an RFID chip versus other potential technologies or even the passport that we all have today. The question that you need to pose and push in this policy making process is, what problem does RFID fix? Frankly, I don't think you'll find one. And frankly, for the Privacy Office to work on it after that choice has been made, that is to create an ID using RFID, has been made, would be too little to late. So, being involved early and asking what problem RFID would fix is a very important role that you can have in the policy making process which, I know, is in its early stages. So again, those are my thoughts. You're welcome to comment if you like, but thanks for hearing me out.

Ms. Cooney: Thank you, and thank you for the suggestion. It is one of the things we are looking at and will pursue further. Thank you.

Ms. Sotto: Thank you very much, Maureen. We really appreciate your presence here and all of your hard work in guiding this committee. Thank you.

All right. Next we'll turn to our subcommittees for reports from the subcommittee. I want to thank our subcommittees. Everybody on this committee is assigned to a subcommittee and works very, very hard to move the agendas of the subcommittee forward. We are issuing papers now at each meeting, and folks on this committee worked very hard to get those papers out and written, and there's an enormous amount of discussion behind the scenes and give and take and push and pull that goes into each of these papers. And so I congratulate all of you for working so well together and contributing so heavily to the privacy dialogue. Why don't we begin with our Screening Subcommittee? Howard Beales is the chair of that subcommittee.

SUBCOMMITTEE REPORTS

REPORT FROM SCREENING SUBCOMMITTEE

Mr. Beales: Thank you very much, Lisa. We have had a busy couple of months since our last meeting, focused primarily on Secure Flight, and you have in front of you a draft recommendation for consideration and adoption. Secure Flight is a very important program, and I think it is an important place for this committee to weigh in. As we were attempting to assess the program, it became clear that there are decisions that have not been made about the program, but decisions that are now ripe for decisions about the structure of the program. So rather than try to evaluate Secure Flight in detail where it was changing, literally, every time we talked about it because different ideas were under consideration we decided that the sensible role that we could play, and that this committee could play, was to set out -- rather than set out a blue print for the program, just set out a framework that would hold it up and hold it together, and that is what we've tried to do in the recommendations that we've put forward.

We have looked at Secure Flight in the context of the existing no fly and selectee list. We have taken those lists as given. There are, obviously, issues that can be raised about the lists and their use, but they are there. They are in use by the airlines today, and what we evaluated was Secure Flight as a way to identify people on the list rather than evaluating the lists themselves. I would say we looked at the criteria about the list for getting on those lists. They are criteria that are developed through the Homeland Security Council. They importantly and, in the documents implementing those criteria, they stress that these lists are not surveillance tools. They are aimed at protecting domestic air transportation rather than surveilling people on watch lists.

We have, in the recommendations before you, five basic recommendations for Secure Flight. First and perhaps most important, Secure Flight should be transparent. I was very pleased to hear the Secretary's talking points about the importance of transparency because I think in Secure Flight, perhaps more than anywhere else right now, that is really a vital concern. The public needs to know exactly what it is that Secure Flight is supposed to do, what information it needs, and what information it is going to use for that purpose. Ambiguity about purposes may provide some flexibility, but it will only feed fears of unwarranted invasions of privacy. We think it's very important that the program should be transparent. It should also be transparent to the airlines about what future information needs might be. Because to the extent airlines have to devise new systems in order to comply with the requirement of Secure Flight, it's important to only be able to do that once.

Second, Secure Flight should be narrowly focused. We think its mission should be limited at this point to correctly identifying individuals in the traveling public who are on the do not fly list or on the selectee lists. We don't think the case has been made for an expansion of the mission of Secure Flight beyond the identification of individuals on those lists.

Third, Secure Flight should minimize data collection. It should limit its collection of information to what is necessary to fulfill that basic mission. At this point, we think there's a solid case for collecting full name and date of birth only. With the passport number -- I mean, that is the information that's available for most people on the lists and that we think is needed to do the job. When a passport number is available as part of a passenger name record because, for example, a flight is a continuation or a domestic connection from an international flight - in those circumstances, we think that passport number may be useful, but we think it is important that Secure Flight should not ask airlines to collect a passport for domestic travel, and it should not seek to obtain passport information out of other data sources like frequent flier records or the like.

Finally, we don't think that a case has been made for utilizing commercial data as a part of Secure Flight at this point. It's not -- it's conceivable that that would happen in the future, but the evidence that's available to date simply doesn't make the case for the benefit of commercial data as a part of this process.

Fourth, we think Secure Flight must provide proactive redress. It should provide an effective mechanism for people who have been wrongly delayed or prohibited from boarding a flight. The determination and any resulting corrections should be made in a timely manner, in a rapid manner and rapidly disseminated throughout the system. The goal should be to avoid, and at the very least, to minimize repeated delays or other adverse consequences to individuals who have been cleared. Finally, Secure Flight must be understood and managed holistically. There are a lot of interdependent systems, not all of them under the government's control, that are parts of the Secure Flight system. It's important, for the system documentation, to address all aspects of the Secure Flight system including those external supporting systems, the policies, the procedures, applications and infrastructures that are managed by people external to the Secure Flight Program Office. The documentation should describe the system as a whole. It may make use of documentation for particular parts of the system that have already been developed, but it needs to demonstrate how key elements are being addressed rather than simply assuming that key elements are being addressed by somebody else.

And finally, we think as part of this managed and understanding this system holistically, that it should be regularly audited, and we think the appropriate entity to do that is the DHS Privacy Office. Those are the recommendations we've come up with in the course of our review of the program. We appreciate all the comments from members of this committee over the last couple of days that I think have helped to make this a better product, and we look forward to discussion and approval.

Ms. Sotto: Thank you. We have a few questions. Sam Wright?

Mr. Wright: Lisa, as you know, at an early stage in the discussion of Secure Flight by the Screening Subcommittee, it was determined there was a potential, and I would like to emphasize, potential conflict of interest as it relates to a subsidiary of my employer. And as a result, I see serving on this subcommittee, I have not participated in the development of today's policy proposal nor will I participate in the discussion of it - nor vote on the proposal. Thank you.

Ms. Sotto: Thank you very much for clarifying. Thank you, Sam. Jim Harper?

Mr. Harper: Thanks, Lisa. This comes as no surprise to Howard, who I was leaning on half the day yesterday, but I do want to express a concern with Secure Flight that's not addressed in this paper. Howard and all the subcommittee members, with great care and energy, considered the comments I had for the paper, and I definitely appreciate that, and the paper is good for what it is. But, I do want to emphasize this one narrow point before we go forward.

I believe the concept of screening comes from the immigration area where people who are undesirable to have in the country can't be apprehended by U.S. officials, obviously, because they're overseas. Screening is intended to insure that they're excluded or apprehended when they enter into U.S. jurisdiction. This is not the circumstances that apply domestically. Suspects of crime or terrorism planning can be apprehended wherever they are, and obviously, they should be. I've compared, in speeches, domestic screening to placing a wanted poster in the post office and then waiting for the wanted person to come to the post office. I think it's much more important to pursue people wherever they are rather than wait for them to come to airports or wherever.

But screening has deeper infirmities that concern me. People inside the United States enjoy a higher level of constitutional production than people do at our borders. Specifically, Fourth and Sixth Amendment rights apply if screening is a process that is used to degrade or deny people's ability to travel, which is a recognized liberty interest. This is more than just an investigative tool. It represents a unilateral accusation, conviction, and punishment for the offense of creating some risk to air travel. All of it weeded out by the Executive Branch of the government, and that's very concerning. So, the paper represents a great deal of work, and I endorse it for what it is, but it would be unfortunate if it put the department in a position to smooth the edges of an ongoing violation of Americans' constitutional rights.

So, I just wanted to put that on the record, my own concerns that aren't addressed in this paper and now are eluded to that fact, that the paper is what it is but not necessarily a full endorsement of screening per say. Thank you.

Ms. Sotto: Any further comments? Mr. Sabo?

Mr. Sabo: Just a quick comment. When Howard was walking through the discussion of the paper, one area he didn't mention was the focus near the end on sort of an overall security risk assessment for the total system. I know it was embedded in the idea of a holistic assessment of the program and the documentation, et cetera. But I think that's important that the little pieces of operation that are external to the Secure Flight Program Office, but are also part of enforcing the controls on Secure Flight need to be assessed. And particularly, as you’re interconnecting systems which already exist with new systems, you expose additional risk. So one of the recommendations is to really do an overall risk assessment of this too total new system even though it may be relying on underlying systems that are already certified and accredited.

Ms. Sotto: Okay. Seeing no further questions. Excuse me. Joe Alhadeff.

Mr. Alhadeff: This is actually not reflected in the paper, and I think it's not reflected in the paper because it's premature to reflect it at this point. But I think as we look at these kind of systems, one of the issues which we have to think about on a continuing basis is, is it actually effective? Is it delivering what it says it's delivering? Because, at the end of the day, the paper is predicated on assumptions as to what the system will do, how it will work and based on test beds, this is the presumption of what it is delivering. In operation, we will have further information as to whether the system is actually delivering what it says because as you do a benefit analysis, if it's not actually delivering what it says, maybe the incursion is greater than it should be for what it's delivering. So, just on a continuing basis, the path forward on this paper is also a reality check of does it deliver what we think it is supposed to deliver?

Ms. Sotto: Please.

Mr. Beales: I think, in response to Joe and also, to some extent, to Jim, I think effectiveness is, ultimately, is a crucial question, and it is -- you know, I guess it is partly a question of what we tried to here was to look at -- was essentially to take the lists as given, and the effectiveness question really goes to how well do we do in developing the no fly list and identifying people who really are a risk. And I think effectiveness is pretty clear at finding people who are on the list through a Secure Flight system that would comply with our recommendations. Whether that actually reduces the risk is a much more difficult question to address, and that is not what we did. But it is a risk based issue, and it is the attraction of those lists as opposed to other possible missions. They're not surveillance tools. There ways to try to identify people that are thought to be real risks.

Ms. Sotto: All right. We'll take one final question. Mr. Hoffman?

Mr. Hoffman: Following up in this discussion that is ensuing right now, this brings to mind a question I had hoped to ask Paul with regard to the Secretary's talking points but didn't get a chance to. If we're not careful, we may fall into the same trap that I think, to some extent, the department can too easily do, which is assessing the problem at hand and stated for us without looking out a bit more and saying what we should really be looking at, what is effective? As Joe suggested, are we asking the right question? In particular, I would like to put on the record the question for the Policy Office. Maybe it could be transmitted back to Paul. How does the Policy Office intend to have more risk analysis based as opposed to reactive analyses done? My impression, from some of the subcommittee meetings, is we've met with, as I stated earlier, bright people who are doing good work, but they're doing work based on a client request. The request from bubbling up from lower in the organization, as opposed to thinking what will be the most effective way to handle a problem. Secure Flight is a good example. It attacks a certain problem. It may not be the best way to attack a problem, but we answered it. I would like to know more from the Policy Office, so this is not really a question for Howard. How are we addressing, in general, risk analysis concerns versus reaction, and how do we look at those and do a true risk analysis based study, as opposed to something that has more parochial concerns?

Ms. Sotto: Thank you, Lance. I will convey that to Paul Rosenzweig, and I'm sure we'll get an answer from him. Thank you. I would like to ask for a motion from the floor to adopt the Secure Flight paper from the Screening Subcommittee.

Mr. Beales: So moved.

Ms. Sotto: Second? Do I have a second? Joe Alhadeff seconded. Thank you. All in favor [A chorus of ayes]

Ms. Sotto: Any opposed? [No response]

Ms. Sotto: Thank you. The paper is officially adopted. Thank you very much. Thank you, Howard. Let's turn to our second subcommittee report. Jim Harper and Joan McNabb share the Framework Subcommittee and will be presenting a draft paper today. This paper has been, by the way, posted on the web site for several months, I believe, for public comment and will continue to be available in draft form for public comment. Thank you.

REPORT FROM FRAMEWORK SUBCOMMITTEE

Ms. McNabb: Thank you, Lisa. Yes, this is working. We had hoped to offer a paper for adoption by the committee, but having discussed it and discerned that there are further comments that many of the rest of the committee wish to make, we're going to hold it over for adoption to the March meeting. What we have today is a draft dated 12/6 that incorporates the comments that we've received since September, both from committee members and from the public due to its posting on the web site. I was -- this document is intended, primarily, for use by this committee in our work in analyzing the privacy impact of the various programs, and systems, and technologies that Homeland Security is involved in. We also see that it may be of use to the department itself and perhaps even to other departments in the federal government in looking at the privacy impact of security related, Homeland Security related programs. I was struck by Lance's comments on encouraging the department to consider the programs from a risk assessment basis, and that indeed is an essential component of this framework we're recommending. It incorporates some basic risk management questions into the process of evaluating the programs because if a program is not going to effectively accomplish its intention, the privacy impact doesn't even come up as an issue.

So, we put the risk management steps even before the privacy analysis in this process. I think I'll let -- Jim, do you have other remarks to make?

Mr. Harper: Joan has summarized well the process to date, and many people have seen the document and had a chance to review it, but we really do want to impress on our committee colleagues the importance of getting your comments. So, in rolling this over to the next meeting, we want to lay out a very, very clear framework for consideration, and so what I would like to do is move a resolution in the committee that at our next meeting we will have an up and down role call vote on the framework document. Comments will be due by February 10th, 2006, and we won't consider comments after that time, but anyone wishing to make amendments can make amendments -- offer amendments at the open full committee meeting. So that's the clear process. We're all here, so I would like us all to know about the process and use the process, and obviously, get those comments in as soon as you can because a lot of people think this is going to be an important and influential document, and we want to take as much comment as we can from our members and the public.

Ms. Sotto: I would just stress one point. This is a living and breathing document. While we do plan to adopt a document with, hopefully, lots of comment over the next couple of months, at our next meeting in March, we do expect that this document is not static, and that it will change over time, so please do continue to look at this document and refer to it, and tell us about your suggestions as time goes forward. I will take questions now. Mr. Hoffman?

Mr. Hoffman: That's okay.

Ms. Sotto: Okay. I have a question. Could you comment on to what extent you used existing frameworks like the OECD principles, the APEC principles, and other frameworks that exist? And I note, specifically, that the sort of standard fair items like notice and choice are not included specifically by name in this document, though there is some -- those concepts are eluded to in the document. There are -- notice and choice are difficult concepts, I think, in the security arena. One we typically do not want to provide notice to folks who are seeking to do harm in this country. However, there are other instances in which DHS may be involved, like FEMA related instances in which notice and choice is an appropriate concept.

Ms. McNabb: The step four -- the analysis of the effects on privacy interests does -- in developing those steps. We certainly did take into account the body of existing, fairly consistent, privacy values in the form of the APEC. What are they? Principles? The Fair Information Practice Principles? The OECD standards? The EU standards? There's a general body that has pretty much the same basic essence and, in fact, all of those points are covered. They're just covered in a different way in step four.

Rather than starting from the principles, it reaches underneath the principles to what we believe are the underlying values and then calls out the principles in the form of questions underneath the values. It's certainly something that one of the things that we might consider doing in the next -- that we will consider doing as we develop it further is to articulate that somewhere. To make clear that there is that relationship to the existing privacy values that are out there -- for privacy principles that are out there in the world.

Ms. Sotto: Thank you. Any other questions? Okay. Mr. Beales?

Mr. Beales: I just want to comment on the use of notice and choice. I think this document reflects a much more productive starting point for thinking about privacy issues and privacy intrusions than was there, the right form notice printed on some piece of paper that no one read. This is a much more productive way to get out the underlying issue of why this matters, and it is not that notice is irrelevant, but it should not be the starting point. We should think about the underlying principles that matter. And I think this document does a nice job of that.

Ms. Sotto: Mr. Hoffman. Did you have a question? No. That's okay. Do we have any other?

Mr. Alhadeff?

Mr. Alhadeff: Just a quick one, and Jim and Joan, this may be something that is done, you know as a kind of a cover note to the document on the web site, so it doesn't necessarily have to be done. I'm not necessarily asking for an answer right now, but I think something that maybe confused some of us in our first round of comments was, perhaps, a misunderstanding or an incomplete understanding of what you guys saw as the scope and application of the document as to how it would be used. And I think, perhaps, a section in the early part that describes that may help people target their comments in a better fashion because, I think we all came at this with a personal understanding of how it would be used which turned out not to be a group understanding of how it would be used. And therefore, geared comments to our subjective view of the document as opposed to, perhaps, a more collective view.

So, I think if there's a way to clarify the scope and application of the topic, it may help make the comments precise in order to meet the deadline you laid out, which I think is very reasonable, and I think the analysis framework is one that allows us to be more proactive, which I think -- it's kind of the same thing Howard was saying in a slightly different fashion. And I think there is a benefit for both a policy and a risk analysis framework which I think this lends. It's just a question of how we use it and how we target the specific language we address.

Ms. McNabb: We would appreciate comments on how you think it should be used, not necessarily right now but when you comment.

Ms. Sotto: Mr. Barquin.

Mr. Barquin: I would like to add one other thing with is -- also in light of the, first of all, the statutory of the privacy impact assessment. I think it would be useful also to see how this document and the PIA process and documents actually would work together. I think it goes back to Joe's comment of how exactly is this going to be used as we move forward?

Ms. Sotto: Okay. Is there another question? John? Mr. Sabo.

Mr. Sabo: I just want to echo that I think, as a guide to the committee, it's valuable. Some of the questions that are less objective and more subjective become harder to deal with, I mean in Secure Flight is a good example. We wrestled with a lot of the implications of the effect and the basis for the list, and the names, and some of the other considerations there. But then in the end, we felt we really had to examine the operation, and the specific procedures, and policies, and structure of the program as presented. So I think, to some degree, it's appropriate, but it doesn't try to do this. Quantify how you can address some of these points and principles. I mean you can't -- in some cases, there will be huge civil liberty implications, but not necessarily much a committee such as this can do about them because it is a congressionally mandated program, and we're reacting and being asked to look at the privacy implications of a program.

So, it's just a comment that -- it covers a lot of breadth, and there's a lot of potential depth, but there may be issues the committee wrestles with that can't be addressed. The other related issue is it seems to be focused on, and I know it doesn't confine itself to that, but it focused heavily on new initiatives, new programs rather than necessarily programs that have been in place that the committee might want to look at retroactively, and that's where you can really not necessarily deal with estimations of impact, but you can really deal with measurable results. And I know this doesn't conclude that, but I think the tone of it seems to be more in terms of new programs, and that may be something to think about modifying when we provide comments back to you.

Ms. Sotto: Thank you, Mr. Sabo. I want to, particularly, thank Joan and Jim for shepherding this paper through. You can imagine that this is not a monolithic committee. If we are 20 people on the committee, we have 22 or 23 different viewpoints, and Joan and Jim have been extremely flexible in taking comments, and we very much appreciate that. Thank you. Next -

Ms. McNabb. We do have a resolution before the committee, do we not?

Ms. Sotto: Okay.

Mr. Palmer: I would like to move the resolution to make sure that we're all on board with this. That again, we will have an up or down role call vote at the next meeting, comments due February 10th, 2006, with no consideration of comments coming after that, let's say midnight. But, of course, people can offer amendments to the final draft we produce in open committee.

Ms. Sotto: Jim has moved. Do I have a second?

Mr. Hoffman: Can I make a comment on the resolution or discussion? I'm wondering, since it's going to be a resolution that would then bind us, I just would like us to explore whether there's a mechanism we could use in that process for the comments that are submitted by the members of the committee to be shared with the other members of the committee so we learn from each other as we're reading through the document.

Ms. Sotto: We're not permitted pursuant to the FACA process, to share comments with members with the entire committee unless we share with the public. Now I think that is a great thing to do, to share with the public. But to the extent that thoughts are inchoate or not yet fully formed, you may want to discuss them with a smaller subcommittee before opening them up for public viewing.

Mr. Hoffman: So can I ask for a different amendment to the resolution then which would be for the chair and for the chairs of the subcommittee to explore with staff, ways within FACA that we could, directionally try to approach being able to share as much as we can, legally the feedback that is submitted. Possibly that might be sharing some of that feedback with the subcommittee chairs, for example, so that there can be some sharing of information, and there is a dialogue instead of unilateral transfer of comments?

Ms. Sotto: I think one way to get to that, David, is for folks on this committee who are particularly interested in working through the gritty issues, to please submit your names, specifically, to Becky Richards and to Toby Levin, and we will form a small working group to the extent we're permitted by law, and we will explore that to discuss particular comments with Joan and with Jim. Okay. Let's continue to work on your resolution. Do I have a second?

Mr. Alhadeff: Second.

Ms. Sotto: Joe Alhadeff seconds. All in favor? [A chorus of ayes]

Ms. Sotto: Any opposed? [No response]

Ms. Sotto: So moved. Thank you very much. Charles Palmer. Could we hear from you about the Emerging Applications and Technology Subcommittee?

REPORT FROM EMERGING APPLICATIONS AND TECHNOLOGY SUBCOMMITTEE

Mr. Palmer: Certainly. Thank you, Lisa. Since the last meeting we met, subject to all the rules, via teleconference, and we also met with members of the S&T Directorate. The Science and Technology, thank you, Directorate to try to find out how we might better work with them and understand what they're doing and so on, and not surprisingly, we found them to be very highly skilled collection of folks, very informed and also very busy collection of people. As I mentioned earlier, we found them to be, however, in a more technical or advanced development kind of role, hurry up and build it, hurry up and figure out how to build it kind of role rather than a policy or prescriptive role which they hardly have the time to do what they're doing now much less to take on another role.

And it's our opinion that there is a clear need for such guidelines for the applications of technology and emerging applications inside DHS. So, to this end, we too are building a paper. Perhaps it won't be as controversial as others. Our first goal is, by the next meeting, to have ready for acceptance a draft, final draft shall we say, on RFID technology. It's a very broad field, very active field, very busy, and unfortunately, RFID technology, despite its appearance in all of our lives to one degree or another, is one of the most misunderstood and misapplied technologies on the planet. It's low cost, apparent low profile, out of sight out of mind, low interference with our daily lives, it makes it very attractive, but also those very same techniques or capabilities also make it a privacy issue, or a concern.

It does have its limits. It is not the silver bullet of the mid 2000's or whatever we call this decade. It is attractive, in some cases, over its alternatives. In some cases, there are no alternatives, maybe the idea of cargo. But it does have its limits, its capabilities and uses for which it would be appropriate and acceptable, and our plan is hard to describe those.

The applications that make perfect sense, that are in place today and the other applications that are in place or almost in place that are a little misguided might benefit from some advice. So we want to define the straightforward applications of how you decide when RFID is appropriate or not, when it is not quite the silver bullet, what you might need to do in addition to RFID, to shore it up a bit. We do not plan on providing a tutorial or RFID that we are certainly aware there's a very large volume of data on that, Garfinkel's book, not to plug it, but it is relevant at the moment. It just came out.

Any other technology, the applications that make sense, and we want to make sure that when RFID is selected, it will be used in the right way. Paul mentioned the cargo concern. Clearly, RFID plays a role there. However, since the privacy implications there, as my colleague Jim pointed out, the privacy implications are limited in most normal uses of cargo. We won't be addressing that directly. However, in the spirit of the full name of the full committee, which includes the integrity word, we may include some comments on when RFID technology and the integrity issues come to play and in non-personal privacy issues, but we're not going to dwell on that. This paper is primarily on the personal information concerns.

Like I said, we hope to provide the guidelines, clear statements of how accurate it can be because RFID, again, is good for what it is good for, and that will be a common theme throughout the paper. It is not always as accurate as you might think. Discussions of the secondary effect and the enormous amount of data, it's one thing to RFID, everything, and it's entirely another to deal with the flood of data that it will produce, and a general means of weighing the value of these applications against the problems or potential impact to data integrity and privacy concerns. We will be limiting our focus despite, as geeks, our tendency to think, well let's solve the problems of the world. We will be limiting our focus to DHS applications.

So, while the paper may be of use to other organizations inside the government and the public sector, our focus will be, indeed, on DHS. We plan on -- we've already made assignments. Everybody has their working orders for the next several weeks. Granted, the holidays will pose a challenge, but I know that the team is up for it. So, I look very much forward to the next few weeks and, certainly, the next meeting when we present the paper for adoption.

Ms. Sotto: Thank you very much, Charles. Any comments on what the Emerging Application Subcommittee is planning? Seeing none - let's move on then to our fourth subcommittee, the Data Sharing and Usage Subcommittee which is chaired by David Hoffman. David, please.

Mr. Hoffman: Thank you, Lisa. The subcommittee currently has three bodies of work that are in process. The first being the examination and analysis of the uses of commercial data, and by commercial data, we mean large aggregations of commercial data generally. The second is an examination of the privacy -- the department's privacy offices, privacy reviewed processes, and the third is an examination of information sharing issues, both interagency and intra-agency. Before I describe each of those, there are a couple of comments that cut across all of them.

First, I would like to personally thank the staff for an incredible amount of work and being extremely forthcoming with us, providing us information often on unreasonable time lines, and at last minute requests. It is greatly appreciated. I can't express, strongly enough, to the public how well I think we, as U.S. citizens, are served by the staff who we have in place and being able to see them actually at work is a fantastic thing.

The second comment I would like to make is to hold out the work of the Framework Subcommittee, even in draft form, as an excellent body of work that is already being used by several members of our subcommittee actually as a guide on how to conduct the analysis of these different issues. We actually had a subcommittee member mention they were having great difficulty getting started on a body of work until the most recent draft came out, and it really helped to move that forward. So many thanks to Jim and Joan for pushing that forward. So, taking each of the three silos in turn, I will take them in the order in which the work is furthest along. The first would be our pursuit of the analysis of uses of commercial data. We have published -- it was ratified at the least meeting, our paper on the use of commercial data for reducing false positives. That is now published in final form on the Privacy Committee's -- on the committee's web site, and I would like to highly encourage members of the public, once again, to submit any comments you do have about that paper. We are continuing to listen to all comments that come in there. We are greatly pleased to hear, from the staff and from other members of the committee, that the paper has been useful. We would like to continue to make it as useful as possible, and we have committed in the past, and we will commit again, that if comments come in that to point out that it needs to be modified in any way, we most certainly will do that, and we will release a new draft.

We also, at the same time, are trying to broaden our analysis of the uses of commercial data. The issue of whether commercial data should be used to reduce false positives is a fairly small and concise issue that allowed us to examine the issue. I think it was very helpful. What it did is it allowed us to see what the different impacts are. It was a framework of analysis now that we can take and move to the greater idea of uses of commercial data. There is work in process to be able to do that. The next steps in that will be to draft an outline, which we intend to make public for comment, that would then result in an overall paper on uses of commercial data. And so, as we continue work on that outline, any of the comments that people have, not just on our previous paper but about uses of commercial data, generally will be extremely helpful to the subcommittee.

The second silo of work is around the department's privacy review processes. The staff was extremely helpful in making available to us information about their process of putting in place the privacy impact assessments, and what those are going to look like and the process that we use of making sure that those are integrated into the program development cycle that the department has. I have to say, from our initial analysis, the subcommittee has been very impressed with the excellent work of the staff. We have some follow up questions that we're going to be providing to staff to get more information, and we expect to be authoring a paper that will provide a review of the overall issue of privacy review process that will, likely focus on the privacy impact assessments. But, will also focus on a process that the office is putting in place around the privacy threshold analysis that happens earlier in the development cycle not when all of the decisions have been made about how a program should operate. Which is really when the privacy impact assessment happens.

The third silo is information sharing. This is something that is not as far along. We have spent most of our time, up until this point, really getting an understanding of the legal basis for information sharing. Within the information sharing, within the government interagency and intra-agency, we now are ready to move that to the next step. We believe what we would like that to be is an examination of information sharing in the context of a very specific example so that we could make this very practical. The recommendation has been made that that example could be information sharing that happened as a result of Katrina, and information sharing that happened as a result of FEMA's efforts there. We're going to continue to explore with the staff, whether that really is a useful example to bring out the issues. If it does prove to be, then we will have a paper that will examine it in that context. That's all.

Ms. Sotto: Thank you very much, Mr. Hoffman. Any questions? Mr. Leo?

Mr. Leo: I just have a question for David -- a request rather. Recently, within the last month, there have been some published reports on the use of commercial databases by the government, et cetera. In one article, which I'll give you at the break of this meeting if you do not have it, it talks about the current interest of Congress in looking at rules, perhaps strengthening rules with regard to the governments use of commercial data. One specific Bill, the Personal Data Privacy and Security Act introduced by Senator Arlen Specter of Pennsylvania and Patrick Leahy of Vermont, as an example. Is it possible that that group working on commercial data could keep the committee, as a whole, informed on where Congress is at particular points with regard to this commercial data used by the government?

Mr. Hoffman: I'll have to explore that with the chair. I'm not sure that the subcommittee feels that it should be the subcommittee's responsibility to understand where Congress is acting instead of looking at the practical impacts of the use of commercial data and providing recommendations on how those should be integrated into the department. But, I'm open to the -- it's the first I've considered that, so I do want to think more about that, and I would love to hear what other people think.

Mr. Leo: I just want to clarify. I wasn't requesting for us to take a stand or to make a recommendation to the hill. I just -- I felt if we were informed, it might have impact on how we, ourselves, address the commercial data question. So, it is an informative request as opposed to, perhaps, an active request. Thank you.

Ms. Sotto: That's certainly very easy for us to comply with. We will take that under advisement. Thank you very much, Mr. Leo. I want to just echo David's thoughts about taking comments from members of the public. We're very interested in your comments. We read them. We absorb them. We discuss them. And often, very often, those comments are reflected in our final paper, so please keep those cards and letters coming. Any other questions? Yes, Mr. Barquin?

Mr. Barquin: Yes. One quick one for David. In so far as we're looking at Katrina as a possible scenario to look at this information sharing, and you had mentioned intra and interdepartmental, but in the case of Katrina, so much was also involved with inter-government, state, local as well as with NGO's such as the Red Cross, et cetera. Are you looking at that broadly enough to make sure that a --

Mr. Hoffman: I think that is an excellent comment, and I would like to take it down that I think that it's something we should examine whether that is the first step in the analysis or we start with interagency and intra-agency then build on to that, but that it sounds like something that would be necessary for us to do.

Ms. Sotto: Mr. Hoffman?

Mr. Hoffman: Also following up Ramon's comment, if you do go forth with your Katrina investigation, I hope you make it not only retrospective but prospective. It would be a great opportunity, not only to look at the local, state and federal response to Katrina, and lessons learned, but also tie into an immediate thing that Joe mentioned in terms of, I think, avian flu or something like that because it has many of the same characteristics.

Mr. Hoffman: I would agree with that. I think the value that we saw in taking an event that was still very fresh in everyone's minds and gathering data of what has happened was that we could then take hopefully, lessons learned from that and provide recommendations, prospectively, on similar incidents that could happen and what should be done in that case, and I think that's an excellent example of one that would be, if I understand the comment.

Ms. Sotto: Mr. Purcell?

Mr. Purcell: Just to, very quickly, to follow on to that Lance, that the word investigation would not be appropriate. What we're hoping to do, is to illustrate, by using some case study, what does happen in the real world, and how preparedness can actually benefit the committee and the Privacy Office, and DHS more broadly by looking forward to using those illustrations, using those case studies, looking forward to other events like influenza, a pandemic, and any other event to help people to begin to better understand what the proper channels are, what the processes are and, perhaps, hopefully, to have those in place prior to the event.

Ms. Sotto: Mr. Alhadeff?

Mr. Alhadeff: Yes. Just as a clarification because I don't think anyone should expect that we're preparing the disaster recovery plan for avian influenza. What we are looking at is what may be guidance as it relates to information use and sharing which is essential to be part of a recovery plan. So it's, perhaps, some principle. The output it may be in the form of -- you know, based on these lessons learned. It would have been facilitated if these things could have happened, and information sharing among these agencies or these groups can be facilitated, but should occur under a set of principles which assures that the sharing can occur but the rigor is not lost just because you're in the situation of an emergency.

Ms. Sotto: Thank you for clarifying. Okay. Seeing no further questions, we will take a short break. Let's reconvene here, please. Please be in your seats at 10:45. Thank you.

[Recess]

PANEL DISCUSSION: DATA ANALYTICS IN THE PUBLIC SECTOR

Ms. Sotto: I'd like to call the meeting to order, please. Could the next panel please come forward? Thank you. I'd like to welcome our next panel. Let me introduce these speakers. We will start, please, by hearing from Dr. Xuhui Shao. Did I pronounce that right?

Dr. Shao: Yes.

Ms. Sotto: Okay. Thank you. Dr. Shao is Vice President of ID Analytics where he currently leads the analytics team that's responsible for developing core technology and advanced analytical solutions for identity fraud. Dr. Shao has, for the last decade, been doing research and development work in machine and computational intelligence in both academia and in industry. Prior to joining ID Analytics in 2002, Dr. Shao was a key member of the Falcon Technology Team for credit card fraud detection and a lead scientist in the technology development group at H&C Software which is now Fair Isaac. Dr. Shao.

Dr. Shao: Thanks for inviting me to speak in this venue. I'm very excited being here. I think the purpose of us being here is to discuss what analytics is and how data analytics can be helpful in the government sector. In ID Analytics, we are a group of scientists, you know PhD's, spending the last three and a half years building analytics technology and trying to solve the problem of identity fraud, identity risk management. Which is not unlike the problem they're facing, the Department of Homeland Security today, in antiterrorism and other homeland security related issues.

And first of all, what is analytics? I think in the simplest form, you can define analytics in kind of a two step approach. The first step is to generalize the patterns -- the statistical significant patterns, from a large amount of data into a statistical model.

And the second step is to apply this model to prediction, what we call a deduction step where the model is applied to make predictions. So, it is important to consider both steps because no matter how good the model is in describing the past behaviors in a data, it is -- the most important thing is to assess the prediction capability of future instances that the model has never seen before. And I'm glad to hear that one of the subcommittees has written the paper on false positives. I haven't read the paper yet, but I will after this. And I think this is one of the most important concepts in assessing analytics technology is to understand the impacts of false positives in identity risk -- identity fraud problems. The false positives is simply an inconvenience to consumers, but in homeland security, the false positives we're talking about are human beings being subjected to unnecessary intrusive hassles and other kind of privacy invasions.

And so it is important. It is the role of analytics to address this problem, to reduce the false positives, and it is a hard problem. Because one of the trends in recent years is the growing amount of data. Every company, every Fortune 500 company, probably has terabytes of data, and it's growing at an exponential rate. It is not only the amount of data but also the growing complexity of the problem, especially in identity risk area, that the complexity of the problem and also the dynamic nature of the problem requires us to build dynamic models understanding the changes and evolution of identity. Which leads to my next point is that it is -- identity problem is a big problem just like – false positives that no single party can see the whole picture. Therefore, to assess the full picture of frauds or terrorists, and this leads to the complexity of identifying the problem and therefore, building the model to detect any suspicious fraudulent behavior -- be it's identity fraud or terrorist behavior. And if you know -- if you know the frauds, you can build any models. There are a lot of methods to build models to detect any behavior, but what if you don't have a lot of examples? What if you only have 19 hijackers and among millions and millions of normal passengers or travelers or other normal behaviors?

So what we have, a group of scientists, as I mentioned before, building the last three and a half years is not only a set of unique techniques but also, we have gained valuable insights into the issues of not building models without overly relying on past negative examples. There are many attempts in the industry of building large negative files, but all have failed because this dynamic problem and the growing complexity of the problem. And so instead, we choose an anomaly detection approach in which we try to understand and establish the normal behaviors by understanding what is normal. Then we can detect what is not normal, therefore, risky behaviors, be it the likelihood of an identity involving fraudulent behavior, or be it the identity involved in terrorist behavior. So, this is very important. That is a very different approach than the traditional data analytics approach by relying on understanding the normal behavior rather than try to understand a very few examples of abnormal behavior.

And the last point I want to make is how analytics can help. One example of that is in the area of synthetic identity. For example, there's, I think, one area that needs improvement in the department of -- in the area of homeland security is the terrorist watch list. And someone like Osama Bin Laden probably won't travel to this country under his real identity. And so, therefore, in a watch list by relying on just matching to a known lists of terrorists would not be terribly useful. The people will probably choose -- it's safe to assume that people like Osama Bin Laden or other terrorists would probably travel to this country using fake identities, probably not even someone else's identity, probably a completely fabricated identity. In our experience, we find that, for the fraudsters, it's a lot easier to use fabricated manufactured identities, because there's no risk of being flagged by or exposed by real victims. Because of this information age, everything, almost everything can be done electronically. It is pretty easy to - - it's much easier to create an identity than to steal one from somebody else. And so by matching or detecting data inconsistency is not very effective in catching synthetic identities. And we have some experience in that. I would be glad to discuss how we can apply analytics to deal with problems such as synthetic identity, which I believe is a big area and also in homeland security. So, thanks for inviting me here, and I would be ready for questions.

Ms. Sotto: Thank you very much. I think we're probably going to have a few questions. I will start by asking whether you are currently -- whether ID Analytics is currently working with the government on synthetic ID fraud issue? And if you could comment on that, obviously without revealing SSI, but if you could comment on either you're working with the government on synthetic ID fraud or in other contexts with DHS in trying to combat terrorism issues? And in what context you're doing that? And if you're not working with the government, in what context you are working in trying to identify the abnormal behavior that you've mentioned.

Dr. Shao: Okay. We're not currently working on any specific contracts with the government. When I talk about synthetic identities, mostly based on our experience, we're working with the financial institutions in the problem identity fraud and identity risk management. But we have written some white papers in this subject matter, and one of my colleagues is sitting in the audience. Tom Hershowitz has talked to, and is ready to talk to more folks in DHS to further this discussion and seek opportunities where we can help.

Mostly my experience in analytics is based on the commercial usage and helping the financial institutions to reduce identity fraud and help the consumers.

Ms. Sotto: Thank you. I see synthetic ID fraud as a huge risk in this country with respect to national security, so I would hope that DHS is thinking about that as well. Mr. Alhadeff?

Mr. Alhadeff: Thank you and you know you've mentioned the role that ID Analytics plays, especially across a number of the large players in the financial services sector. And I was wondering if you could comment in that, to what extent you are able to use both your predictive and deductive techniques in distributed systems or whether the information has to be centralized before it actually can have those -- the analytics tools run against them?

Dr. Shao: Sir, we have both forms. We have both. In ID Analytics, we believe the value of trusted networks. And basically we build this network data in a very limited purpose which is identity risk management and combating identity fraud in a very highly secure environment. So, it is important to have this trusted network so that we can explore as scientists, and we have all the data available to us from diverse sources. We can detect very subtle type of patterns of anomalies and suspicious activities, and we also operate under some of the -- in a more disputed manner, where we work with dozens of data vendors by collecting and sharing data either in an offline environment or in a real-time environment -- in a distributive manner. Dynamically assemble data and to detect any established normal patterns as well as detecting any deviation from the normal pattern.

I think I've read in techniques, for example, Jeff wrote some materials on anonymization. I believe that certainly there are different applications of these kinds of techniques. But in my experience in identity fraud, it is important to capture the raw, unadulterated information from a client. For example, we don't encourage our clients to normalize, so to speak, the data because that removes information from its raw form, therefore would have a limited ability to detect subtle patterns.

Ms. Sotto: Mr. Barquin?

Mr. Barquin: One of the things that this committee has discussed and actually, we've produced at least that paper is the use of commercial data. And government, as you know, is much more constrained than the private sector is in terms of what it can do directly with a lot of these commercial data vendors, plus there's been a very significant amount of negative visibility that a lot of these data aggregators. And I guess the question is, if you were all of a sudden asked to come into government and try to apply your analytics techniques to try to solve some of the very, very important issues that homeland security is dealing with, what kind of arguments would you make in favor of the use of commercial data and what kind of protections, how would you frame it to make sure that it was not misused in terms of privacy invasions?

Dr. Shao: Sure. That's an excellent question. I can only draw upon my experience at ID Analytics, our company, ID Analytics has experience in this area. We build this trusted network to serve our clients. They want to solve this problem of identity fraud just like the Department of Homeland Security wants to solve the problem of, you know homeland Security. Where we have successfully built this trusted network model where we apply -- we collect the data for the sole purpose, for a very limited narrow purpose, of solving identity fraud problems. And what we don't do is we don't sell data, we don't transmit back the data, and we only send back the score that indicates the likelihood of this identity involved in fraudulent behaviors and also the reason codes, why it is so to our clients. And that to help them to guide their identity risk management process without having to share the underlying data ever back to the clients. So, I believe this same model can work for the government where we can apply data analytics to this problem but only -- first of all, in a very limited purpose and in a very secure environment. And second of all, never share back the data.

And the government doesn't need to know the underlying data but only can get the score and get the reason code, and therefore, solve this problem. Does that answer your question?

Ms. Sotto: Mr. Harper?

Mr. Harper: At the outset of your statement, you suggested essential similarities between identity fraud problems and the government, the government issues which I assumed -- by which I assumed you meant terrorism detection, terrorism planning detection. And I appreciate the model you described for how it works. Induction step is to collect data on the target activity, and the deduction step is to use the model you developed to find the future instances of that behavior. But the difference, to me at least, is obvious that terrorism has very few instances that we can study. And the next terrorist attack, as we have seen several times, is different in most respects, many respects from the previous one.

So you move to anomaly detection, and that concerns me. I wonder what kinds of anomalies you think you would best look for, and does that amount to anything better than guesswork?

Dr. Shao: Sure. That's an excellent question. I think that -- definitely I think there are a lot of differences, and there is a lack of sufficient examples in the past that would make this, analytics a big challenge. But I think anomaly detection is precisely the right approach in this application in solving this problem. Because first of all, today's methods, for example, security screening at airports, or subject everybody through those security measures creates, already, large number of false positives. And I think the analytics can help reduce the false positives. And second, your question about false positives -- about anomaly, concerns about anomaly behaviors were not, in my experience, for example, we always say -- you know, before I build identity fraud models, I spent many years building credit fraud transaction models. One man's behavior is another man's suspicious behavior. I use my card several times everyday, but some people only use it once a month or twice a month, and there isn't universal anomalist behavior. It is important to consider everything in the right context. And so when I say anomaly detection, I mean establishing the normal behavior under every specific context, and therefore, in every context to understand what is normal. Therefore, we can detect what is out of the character of the behavior and what is out of this context behavior. And same time, many action can have a normal legitimate explanation and can have a normal legitimate context, and so we can define the normal legitimate context for every action. If that is not in existence, then it becomes more risky and more suspicious.

So, I understand your concern, but that's precisely the problem we're trying to solve be it in a credit card fraud or in identity fraud. And furthermore, I think -- the reason I say there's a lot of similarities, I do believe, like the example of synthetic identity, that identity risk is a big problem -- a big issue in homeland security like I mentioned the terrorists probably won't travel or do things at least under their real identities. If we can assess the likelihood of who they say they are, people being who they say they are, then we can be much more confident in applying full on security measures and investigations. So there's a relevancy there as well.

Ms. Sotto: Okay. I'm going to take one more question. I'm sorry to have to cut off questions, but we need to move along. Mr. Purcell?

Mr. Purcell: Quickly, if I could. The complexities abound obviously, and once you get through the behavioral complexities within a limited market, like a domestic market. We have the additional complexity of an increasing ease of movement globally. And so we have cultural identity standards whether they're naming conventions, whether they're identity documentation, whether they're just immigration not necessarily with a one stop from one country to another but, perhaps, with several stops from an origin country to an interim country to another interim country and finally, into a destination country over a period of time.

First question, do you handle these global issues of cultural identity as well as governmentally based identity in a multi-cultural society? And secondly, what are your findings in that, and what advice would you give to us, as committee members, about thinking more broadly than just the context of a U.S. driver's license or a three name convention with a middle initial that generally is not used, that kind of thing?

Dr. Shao: Thanks. Yes, we have some experience in expanding into other geographic locations and solving similar problems. What we have found is that you have to develop a set of technology that not depend on specific elements of identity or elements of the problem you're trying to solve, but rather, develop a set of techniques that rely broadly on a wide variety of data elements. I cannot say, specifically, what data analysis is needed because in any analytics exercise, there's a research face and there's an applications phase.

In the research phase we consider more widely data elements, but then we determine what data elements are relevant and what ones are not relevant. And in the application phase we can narrow it down. But certainly we can apply the same techniques in different countries. For example, we tried in the United States as well as in the United Kingdom and Canada -- we would look at different countries. And there are a lot of similarities in terms of analyzing the identity risk, not as you build the techniques, rely upon very broad data elements instead of just focusing on something like very unique locally, like social security numbers. This is only in existence in this country. Then we have experience that the technique works in other kind of use in cultural identity.

Ms. Sotto: Thank you very much, Dr. Shao. We really appreciate your speaking with us. Our next speaker is Mr. Jeff Jonas. Mr. Jonas is the Chief Scientist of IBM’s Entity Analytic Solutions Group and an IBM distinguished engineer. Mr. Jonas is responsible for shaping the overall technical strategy of next generation identity analytics, and the use of this new capability in the overall IBM technology strategy. The IBM Entity Analytic Solutions Group, that is a mouthful, was formed based on technologies developed by Mr. Jonas as the founder and chief scientist of Systems Research and Development, which was acquired by IBM in January of 2005. Mr. Jonas is also a member of the Markle Foundation's Task Force on National Security in the Information Age and serves, presumably served, with Tara Lemmey who, unfortunately, is not here today. Thank you very much for joining us.

Mr. Jonas: Thank you. Good morning. I appreciate the opportunity to be here to testify. I've spent 20 years building and employing systems. I'm more of a practitioner than a researcher. About four years ago, I made my first footsteps out here to the east coast, and prior to September 11th, the government's interest in my work was in finding insider threats from those within. And of course, post September 11th, I find our technology being used in counterterrorism and national security kinds of engagements. Over these four years, I've had an increasing awareness about the importance of privacy -- from privacy-enhancing technology to policy and guidelines, government oversight and so forth.

And with this context in mind, I thought I would just mention four observations and recommendations. Roughly, these are going to be the importance of directory-based information sharing, anonymization, immutable audit logs and the limited role for data mining to predict the terrorist intent of a few.

I'm just going to put a little meat on the bones of each of these. In the area of information sharing, everyone loves or wants to be involved in information sharing, and they basically said, “go ahead and send me all your data”. But the challenge is everyone wants to protect the data they have. I see three models of information sharing, two of which really won't work. One is everybody has to take all of their data and give it to everybody else. But you can't keep it current and there are many other problems. Another requires everybody to ask everybody else every question everyday. Otherwise, how would you know with whom to share the data? It just does not work either. The third model, which I'm finding quite practical, is the use of directories. This is much how libraries work. One does not roam the halls to find a book. Rather, one goes to the card catalog (i.e., the directory), and the directory provides you pointers. So, each data holder gets to hold their data and know who's asking for it, and better yet it is discoverable because somebody has gone to a directory. And this is a model that I think can work. But questions arise from this model: What are the policies around such a directory? Who will hold the directory? What data do you put in the directory? How do you govern how people use the directory? This is where our thinking needs to be directed.

I spent the last four years working in the area of anonymization and how to do deeper analytics of data using only anonymized data. I think there's some extraordinary promise in the area where data can be analyzed in its anonymized form and yet still yield a materially similar result as compared to clear text analysis. While there are many benefits to this approach, one might be its ability to reduce some of the requirements of Section 215 of the USA Patriot Act, which enables the government to request all data held by an organization, not just the data about somebody for whom there is a specific record.

Through the use of anonymization, one could find out -- or a government could find out -- what three records to ask for and then get a subpoena for the three records. This anonymized information sharing model, I would submit, is more in line with the Fourth Amendment's "reasonable and particular" test for lawful search and seizures. When systems are used by governments that lack transparency, immutable audit logs become particularly important. Immutable audit logs involve the ability to ensure that as users make queries upon the system that their searches are recorded in a way that are immutable or tamper resistant. I have a lot of hope that these will come into existence.

And finally, based on my experience in building marketing systems in corporate America in the billion row category, I am of the opinion that there is insufficient data to look at behavior alone to determine who is going be a bad guy. And while direct marketers have spent billions of dollars to get really good at predicting the intent of a few to buy a product, they still can only raise direct marketing rates from two or three percent to maybe six. Well, a six percent response rate means you have 94 percent false positives. So, I see this as problematic from a civil liberties standpoint when using these techniques to find a few bad guys. But this is not to say there's no use for data mining. For example, I see value in an area I refer to as predicate triage. To illustrate, if you have a list, say a large list of people in the United States who are on expired or illegal visas, you might ask yourself who on that list you might want to allocate investigative resources to first. And in that circumstance, you already have a predicate list. Here you could use data mining to determine which 100 people one should be working on this week. So those are four thoughts that I thought I would bring to the committee, and I'm glad to take some questions.

Ms. Sotto: Thank you very much, Mr. Jonas. That was quite intriguing. Mr. Hoffman?

Mr. Hoffman: Mr. Jonas, one thing I take away from your presentation is that anonymization has much more promise than data mining, if I had to generalize. And I wonder if you could expand, just a bit, in terms of how, for example, DHS might be able to use anonymization and then, in other words, go after anonymized records and then reconstitute using trackers or whatever other techniques used to put things back together, to get the information they want? And also if you have any thoughts on the effectiveness of this or lack of effectiveness when you get into a real-time requirement?

Mr. Jonas: So, I would like to use the Terrorist Screening Center as an example here. They produce the consolidated terrorist watch list. They, to my knowledge, do not post that list on a web site, and they do not provide that list, for example, to a cruise line. And the question is, in protecting themselves from ill deeds perpetrated against them, is the cruise line and the rest of corporate America, inclined to then send all of their data to the Terrorist Screening Center? Well, currently, based upon what I know, this is not the model. All of the data is not being flowed one direction or the other. The hope of anonymization is that an organization, like somebody that is managing a government list, could anonymize it and provide that list either to a third party or an organization that is trying to protect their bridge or nuclear power plant or whatever. And then they would not have the ability to observe who is on the list. In fact, they could ensure their employees are not on the list. And if an employee is on the list, it would match while in its anonymized form. It would notify the holder of the list that there was a match, and now the holder of the list, in this case, the TSC, would know the specific person about whom to prepare a subpoena request. This technology has come of day. Though this technology is in its infancy, it is really working. And we're seeing governments interested in this, in fact, sharing data with themselves in anonymized form.

It might be a surprise to Joe Blow on the street, but an organization that deals in secrets may have one unit three doors down that doesn't communicate with the other group three doors up. So if one group is working on counter-proliferation and one is working on counterterrorism, they both have an inability to discover when they're working on the same record. And this means that these kinds of organizations, with all these silos, can avoid the Go Fish game they currently play – where everybody must ask every smart question every day. So, anonymization is a technique they can use to share data with themselves, in the same matter that I mentioned, to discover when two different compartments, three doors down, have a record in common and then talk just about that record. I hope I answered your question.

Ms. Sotto: Mr. Sabo?

Mr. Sabo: Dr. Shao mentioned and you also touch on, I think, when you talked about directories, the importance of policies and when you move in information sharing systems, then security policies which help protect privacy are really critical, and that becomes the identity of the individuals, access to the directory itself, the identity of the individual managing all of that. So as you build bigger distributed access systems and directories for information sharing, then it seems to me that these problems of security compound themselves. So, in a way, I think -- I mean, you touched on the important point by saying policies are important -- obviously, implementation of the policies become very important, but you didn't really stress the dimensions of this as you move the bigger distributed systems. And I'm wondering if, from your experience, you could talk about that a little bit?

Again, I tie back to the previous speaker who mentioned they like to work within a trusted environment. Well, the trusted environment is a very difficult thing to establish and control. So, as you move to broader information sharing and collecting personal data about many individuals, that becomes a much harder task. And then when you align that against the benefits you're going to obtain, then you have a much bigger cost benefit and trust issues. So could you just talk a little bit about that security dimension? I would appreciate it.

Mr. Jonas: Great. Thank you. As organizations go to shared data and as their possession of data grows, then it becomes more and more problematic to try to have a federated discovery model where you have to send a query or a search to every party. And so that is why the directory model is a more viable and scalable thing. But I will tell you that the bigger the directory gets, it becomes a target. It becomes at risk for a PII breach. Therefore, my latest thinking in this area is to have anonymized directories so what is in the directory can't reveal the underlying PII. In this way, every record in the directory knows its originator, but it cannot, in itself, reveal the name or the date of birth or address. And I think this is the route of the future. Originally, I conceived of anonymization as a possible improvement in the way watch lists are handled. Now, in hindsight, I think that that is maybe two percent of its market potential.

Finally, a notion I would like to advance is if organizations are going to share sensitive data, employee data or customer data or other PII, and if it could be shared in an anonymized form whereby a materially similar result could be achieved, why would any organization want to share their data any other way? And there's a business segment I believe that's emerging which I refer to as "analytics in the anonymized data space." I think so much more could be done in this area, because I think it is so much more protective of privacy and civil liberties. It significantly reduces the risk of unintended data disclosures. Does it reduce the risk to zero? No.

Ms. Sotto: Thank you. Mr Harper?

Mr. Harper: I found it remarkable, and so I will remark on the fact that you, as an expert in this field and somebody who works for a company that would sell this product if it were viable, tells us that predictive data mining is not viable. I think that is an important thing to hear from you. I want to ask you, though, and sort of compare your comments to Dr. Shao, who didn't fully answer my question about the switch from lacking, what you call, a tracking pattern or a training pattern, the lack of a training pattern in the terrorism case to anomalies. Just does switching to anomalies give you something to work with that is any better than a guess?

Mr. Jonas: Okay. A couple of things come to mind. One is, you know, while there’s a large market for data mining, I'm suggesting that using data mining to predict the intent of a terrorist where you're basically putting the finger on a trigger that is going to cause government scrutiny upon an individual is where I see it as a bit problematic. There's also a definitional thing here about data mining. I consider my life's work in the area of knowing who is who and who's related to who -- more of a link analysis view. This has been popularized as subject based queries versus pattern based queries. Mary DeRosa, here to my right, wrote a great paper for CSIS this past year about counterterrorism and data analytics. For the record, I would direct you to the CSIS piece as a very useful resource regarding these definitional matters, among other things. One in a million things happen millions of times a day, and bad guys don't leave as many transactional footprints. And noting that the data marketers using data mining with a tremendous amount of data can only yield maybe six percent accuracy or predictability, I think, is the key point. And Jim, did I miss another element of that or did I get that? Did that answer your question? Okay.

Ms. Sotto: Thank you. Joe Leo?

Mr. Leo: Very quick. I just want to get into a practical issue for advising the government with regard to the two speakers. Feel free to answer for both of you, but I have a report right here, last month from CIS, an audit from the IG at Homeland Security that talks about identity problems, biometrics and accuracies. Our committee deals with not just privacy but integrity of the data. So in the first part, the report says that there's a lot of problems in identifying people applying for U.S. residency and citizenship and are still vulnerable to fraud because they're using a lot of paper documents that are fraudulent, et cetera. So the IG has made a recommendation to the department to link biometrics to the folks applying for citizenship or residency. Which raises the issue of biometrics and privacy, but it also raises the issue of data integrity which gets to our second speaker, Mr. Jonas, that having directories that are inaccurate can pose even greater problems and an anomaly of data, than collecting data and biometrics I'm concerned about. Here's a practical IG report that talks about linkup biometrics with the document for people to apply for a citizenship or residency. And yet, we have an expert before us that talks about looking at, maybe at patterns and looking at a different way of doing analytics with regard to identity management or fraudulent identity. And then we have the next speaker that talks about using directories and anonymizing the names, and I'm going, well, where -- I haven't heard yet the problems thought with this in a sort of like practical -- a practical recommendation to the government on direction it should pursue. So if you would like to comment on that, I would be appreciative.

Mr. Jonas: With regard to anonymization, the main point is the government is seeking large swaths of data to find a few bad guys by working from watch lists which they cannot release (unlike No Fly or Selectee lists which are released on a restricted basis to the airlines). When policy requirements preclude watch list sharing and where legal mechanisms can be used to collect all of the data that a company holds, anonymization enables one to discover what five records they have in common in a more privacy-preserving manner. So, information transfer contains the fewest number of records. I think that is exceedingly practical. And I think it is a huge step forward in terms of privacy enhancing ways government can get its job done.

Dr. Shao: I want to comment on one thing you point out very important is the inaccuracy of data sources. And we find that there's no single source of ground truth. And so, therefore, we don't want to rely on any single source of data and fall in the trap when the data is inaccurate or noisy or has errors in it. And therefore, what we -- our experience tells us if we rely on broader data sources and rely on building broader behavior patterns, then we can more accurately assess the reliability of each individual data sources entrusting the network environment. And also, I wanted to touch upon that -- I'm sorry that I didn't fully answer -- you know, Mr. Harper's question. Yes, it is true that we don't have a lot of negative examples even though the problem of identity fraud is much better than in the area of homeland security. We do have confirmed identity fraud cases and synthetic identity cases where we can actually link suspicious patterns to the known fraud patterns but even though there is still a lack of negative examples. But we don't have a problem of lacking positive examples. We have lots of people that we know and for years, have been either in financial institutions or have been a loyal customer paying their bills every month, and we know where they live, and response to mail, and everything. And I think, in this homeland security space, I don't know what specific procedures, but I do believe you can establish a set of large number of folks that are positives examples. And therefore, I think with millions and millions of positive examples, we can train any analytics methods to, on those normal and positive patterns, therefore, to avoid the false positives. So that is the approach I would suggest taking, focus on the normal positive ones, not just the negative ones.

Ms. Sotto: Thank you. Mr. Marsh?

Mr. Marsh: Thank you, Madam Chairman. This is a very interesting presentation on anonymization, and as we know, it's being used even more now. It is being used in the intelligence community, which is very helpful. Should we have different standards in those searches? Because a search for a terrorist data who may be planning an attack on a facility is a far greater concern. It may be less stringent standards, likewise, search for a criminal activity, money laundering as opposed to general data gathering that might be done by commercial agencies who are putting this information together that they want to then resell and maybe they have encroached, improperly, on health records or [inaudible]. Should the Department of Homeland Security be over in the latter, which has nothing to do with national security but has to do with the protection of individual rights?

But secondly, over in the area of national security, should there be developed standards that relate to terrorism and other criminal activity in your view?

Mr. Jonas: In my opinion, standards should be developed and should be domain-specific. So, if you're collecting data because you're going to prepare for an avian flu outbreak or, in the healthcare space, to share records so doctors can find one's medical records, then in my view, an anonymized directory would have big advantages, at least the way I've been thinking about anonymized directories.

For example an anonymized healthcare directory enabling health care providers to locate medical records would be mathematically and physically incompatible with an anonymized counterterrorism directory. This is very beneficial from a data reuse or repurposing perspective, because no longer could one snap one's fingers and say, “We're now going to converge these anonymized directories and run the health care data against the counterterrorism data.

This would prevent, by having separate domains, converging those data – at a later date.

And from a consumer and citizen point of view, any time we can eliminate consumer surprise, I think that's a great thing in terms of meeting privacy expectations. So whatever one does in this area, I think it should be transparent, and I think it should be domained. Now the policy question is, what kinds of governance, oversight and immutable logging activity one would apply to counterterrorism versus applying to healthcare epidemiology studies.

Ms. Sotto: All right. I'm going to ask that the others who have questions please hold them for now. Let's move on to our next witness, Mary DeRosa. Ms. DeRosa is Senior Fellow in the Technology and Public Policy Program at the Center for Strategic and International Studies. She writes and speaks on information policy, intelligence reform and national security issues, and is also involved in the Markle Foundation's task force on national security. Prior to joining CSIS, Ms. DeRosa served on the National Security Council Staff as Special Assistant to the President and Legal Advisor. Welcome, and thank you for joining us.

Ms. DeRosa: Thank you. Well, I'm going to approach this somewhat differently from the two speakers before me because I'm not a technology person or really know -- I mean, I guess, over the past couple of years, being in the Technology and Public Policy Program, I've learned some, but that is not my background. So, I want to talk some about policy issues with data mining. And I guess I would first like to say that I -- well, I appreciate you asking me to be here, and I also appreciate what you're doing because I find that, even still, to much on the discussion of data mining is of good or bad, yes or no. And although there's a lot to be said in that area, there is -- the result is not enough discussion of if you're going do it, how do you do it right? How do you do it in a way that protects privacy? When do you do it and what kind of standards? So, I think that is a discussion that's very important to have, and I know that that is what you're looking at. I have just -- I want to raise four questions that I think policy makers should be thinking about when they're thinking about data mining, and then just discuss them a little.

The first question, and these have been touched on in some of the earlier discussions and in your questions. The first is, what kind of analysis are you talking about when you're talking about data mining? The term data mining has been used so broadly. And it is just sort of a short hand for so many things now that there's not a lot of precision when those people are having those discussions. And as Jeff said, there is pattern based data mining, but there are also -- and none of these are actually what the researches would call data mining from what I understand. But there are -- there are a range of types of analysis that come under that title, and there are some, like identity verification, that are really very subject based. And I think when policy makers look at them, they should be looking at how close are they to individualized suspicion, being based on individualized suspicion, which is the kind of inquiry that we're comfortable with in our legal system. So, to the degree they depart from that, I think is where they raise more and more issues. So identity verification which, and again, I'm not a technology person, so I'm probably simplifying this overly, but if you have a name, you have some reason to be asking questions about this person, and you're going into the data to find out whether that identity matches with that name. That to me doesn't seem particularly -- it seems on the scale of things less, raises fewer questions.

Then you've got other types of subject based analysis where, again, you start with a person or a thing or something that a subject about which you have some reason to be suspicious, and you do link analysis or other types of subject based analysis. And then, on the other end of the spectrum, is the pattern based types of analysis where you have some reason to identify a pattern of behavior that is of interest but none of the parts of the pattern might be illegal or improper. They all might be innocent, and so there you're departing, more significantly, from the individualized suspicion, and I think that is the kind of analysis that would raise more significant questions.

Second question, how good is it? How good is the analysis you're doing? And this seems like an obvious question. But do you know the rate of false positives? Do you know if it's subject based? How good is the data that you're using? And how -- and again, this has been discussed by the other speakers, how likely are you to be identifying people falsely? And if it's a pattern base, how good is the pattern? And again, this is something we have talked about a bit this morning. When it comes to patterns for terrorism, the terrorist behavior, I think that the other speakers, or at least Jeff has been saying, said we don't have the training patterns. This isn't these patterns aren't very good. Well, I don't know. And that very well may be true, but it's certainly a question you need to ask. I think there have been a lot of questions raised about how good patterns of terrorist behavior are. There might be other kinds of patterns of behavior that is terrorist activity that they engage in to prepare. The one thing I would have to say about that is just because we can't do it now doesn't mean we couldn't ever do it. And research on good patterns for terrorism should not sort of be thrown out along with the actual implementation of those patterns. But, obviously, you need to look at how good, how good the pattern is. And when you're doing the analysis, how likely you are -- how well tested it is and how likely it is to have false positives.

Third question, how much control or how well can you control the use of the data? And that brings in all of the kind of policy and guidelines issues. Do you have -- do you have -- are you, in using this type of analysis, able to do real-time audit? And this is something Jeff mentioned so that you can do monitoring of compliance so you can have some comfort that things aren't sort of spinning out of control in the use of this analysis.

Do you have guidelines? And this is very important, guidelines for retention and dissemination of the data that you're getting. And just for a moment -- I shouldn't talk about stories in newspapers that I don't know whether they're true or not. But one of the most disturbing things in a Washington Post article about the national security -- use of national security letters and the data that was used in Las Vegas, and then there's some data mining -- pattern based data mining, apparently according to the newspaper, done on transactional data that was collected using national security letters. But the most disturbing thing to me was, then according again to the Washington Post, all of that -- all of the data they collected was retained, and there is no sort of policy for getting rid of it or what to do with it. And that, I think, is one of the types of controls that need to be really looked at. Anonymization, the use of technology to protect privacy and what kinds of efforts are being made along those lines? Is there -- are there access controls or permissioning type technology that requires a person using the data mining or the type of analysis to have a reason that is based on a legitimate mission, and to state that reason? So those are the kinds of ◎ those are the kinds of controls. And before adopting some sort of data mining or analysis, there should be questions about how well are we controlling use.

And finally, sort of related to that, is how are the results going to be used by the people who are getting them? Huge differences between if you're using the results of data mining -- data analysis to do further analysis, to do further investigation, to follow up. And there's a big difference between that and if you're using them to actually make a decision or deprive somebody screening, for example, not letting them get on a plane, or detention, or a job decision. There are big differences for the ultimate use, I mean for the ◎ in terms of intrusiveness, if you're using them only for further analysis and for some ultimate decision.

So I think those are four questions that always should be asked when talking about using some sort of data mining. Other types of issues, the Mission Creep issue is just a huge one, and needs to -- whenever you're instituting the use of a data analysis, policy makers should be thinking about whether there is a check on having that type of analysis bleed over into some other use for which there hasn't been the same kind of debate, and there might not be the same kind of justification. So, those are just some thoughts on questions for policy makers, and I'm happy to take your questions.

Ms. Sotto: Thank you very much, Ms. DeRosa. Joe Alhadeff?

Mr. Alhadeff: Thank you. I guess my question dealt with, I guess it was the first of the questions, and various speakers have spoken about whether using directories, whether using kind of an anomaly model you kind of broke it out into, perhaps, using identity verification or kind of the link analysis versus using a pattern analysis. And I've been struck by it's kind of presented often as a “versus”. And I think if you combine these approaches, you actually get much more than if you use them as separate or even sequential approaches. And that, perhaps, the pattern analysis gives you, albeit, an imperfect predicate data set, but when it can be subject to link analysis and then identification analysis to see if it actually helps narrow down the field of people you're looking at. Because one of the problems in list matching is that the list is going to be, by definition, incomplete. So the concept is, perhaps you can actually find through, especially, the link analysis and relationship analysis which has progressed traumatically in recent years in a blended approach. And I was wondering what your thoughts were on kind of a blended versus a separate approach.

Ms. DeRosa: I think that makes a lot of sense. Again, I'm not a person who can tell you how well the technology works. I know when you talk about patterns – I don't know whether you mentioned it in your talks, but using patterns, not for the ultimate question, but to sort of do some additional analysis. And I think that that would be, for me, significantly less concerning if you're using a pattern to get you more information, and then - but that there is individualized suspicion analysis, I mean question, in the analysis you're doing. So I think the approach you suggest makes a lot of sense to me.

Ms. Sotto: Thank you. Mr. Barquin?

Mr. Barquin: Mary, you mentioned something that Jeff Jonas had also mentioned, but really not gone into much depth and as a matter of fact, yesterday when we were visiting the National Targeting Center, came up, and this is the question of - so relevant -

to who oversees the overseers and the ability then to track control, keep logs of who is querying what. And could you comment a little bit on that and, maybe also Jeff Jonas, use and possibility?

Ms. DeRosa: I think it is such an important question and such an important area that, to speak very generally, I think in the past because so much of the information sharing, and there were a lot more restrictions on sharing of information and use of data that there was less of a need for really rigorous compliance, and auditing, and monitoring, and overseeing. And we don't have the kind of system set up for that that I think that is now very important, and that gets back to the first comment I made that we're not really talking enough about how to do it right. We're still sort of talking about yes or no.

I think that there needs to be a significant focus on increasing -- I separate out -- I'm not sure if I'm using these terms in ways that -- you know, the terms are always very difficult because they mean different things to different people, but compliance from oversight - oversight IG's, after the fact investigation, congressional oversight, very important. But, I think what is at least as important now is to really beef up how we keep track, not so much for purposes of punishing people when they've done something wrong, but keep track of what is going on so you can catch something that is going wrong in the use of the system or use of data before it sort of spins out of control. So, use of real-time audit logs and some manner in which you can check up on those logs in a relatively near time, real-time basis to see if rules are being complied with, and the analysis or system is being used correctly. Those types of programs need to be really emphasized a lot more than we have in the past. I hope that answers your question.

Ms. Sotto: Okay. Mr. Hoffman?

Mr. Hoffman: Ms. DeRosa, I'd like to thank you again for coming and speaking to us today. You mentioned, during your testimony, a need to continue testing and doing research to see if we can find patterns. You might want to restate that to me -

Ms. DeRosa: No -

Mr. Hoffman: -- let me just finish, and then you can tell me. I'm just wondering what kind of data would be used in the testing, and what kind of testing you were referring to? And if we're talking about live data that would either come from within the government or external to the government, what kind of controls should be put in place if we're going to continue doing that kind of testing?

Ms. DeRosa: Thank you for asking that question. Because I probably spoke a little to loosely. I was reacting in part to -- as everybody knows, the whole terrorism information awareness, Total Information Awareness Program and how it was stopped, and there was a lot of misunderstanding. There was a good bit of understanding, but also a lot of misunderstanding of what that program was doing. And in fact, in the sort of out there in the world, a lot of people thought it was an active program that was -- I think there was a lot that was useful there because you can't -- in my view, you shouldn't just say, Can't do it, doesn't work, let's stop looking. And that research for effective patterns that can be controlled and that can be consistent with the need for privacy, that that's research that is important to do. On the other hand, it does need to be controlled. You certainly don't need to -- I mean, I think if you're going to be using transactional data on real data sets, I think there needs to be a huge -- you know, there definitely needs to be control of that. And I would only -- you know, I think you should only do it if it gets to the point where it's absolutely necessary, and you have a lot of controls. I think you can do again, speaking not as a technologist, you can do a lot of research without using the kind of data sets that I think raise difficult issues.

Ms. Sotto: Okay. Any further questions? Jim Harper? Yep, go head. We're fine.

Mr. Harper: Just apropos of the last comment, it goes to a theme I guess I've been working on in my questions so far. I'm looking for a theoretical explanation of pattern based data mining. And I wonder why you would do research, considering the privacy consequences implicit in David Hoffman's question, why you would do research when there isn't even a theoretical explanation for what you're trying to do?

Ms. DeRosa: Well I think, if I understand your question correctly, I think there is the theoretical explanation for it is if you are looking for it you're not always going to find it. Everyone you need to find isn't always going to have done something in the past that will cause them to be suspicious in sleeper cells in other types of activities. And so that there could be benefit to finding patterns of activities that could get at terrorists who are planning to do something who have never done anything before. And again, I mean I recognize as most people who have looked at this, looked at the idea of patterns for terrorist activity have said, we're not there yet, there's just not enough - you know, there's not enough past activity to predict. But all I know, as a non-technology person, is that a lot things we couldn't do before, we are able to do now. And I would be disappointed if we just cut off research on something that could prove useful. Obviously you would need to have, before doing some of that research, you need to have a really pretty good explanation of what you're going to come up with and why it is useful and why you're doing it. And again, I think more guidelines, more controls on all of these activities than we really see now, so it's less of kind of the wild west that are important also in the research area. But I do see, at least a theoretical explanation for how a terrorist pattern could be useful.

Ms. Sotto: Joan McNabb?

Ms. McNabb: I think I understood Dr. Shao to say that the kind of pattern based analysis you do starts with defining the pattern of normal. Can you give -- and then, detecting the anomalies based upon not meeting that pattern. Can you give us sort of concrete or real life example of what you mean by that?

Dr. Shao: Well, as I mentioned before, you can certainly establish a lot of positive examples. For example, we look at financial data. We know that, based on the financial relationships with each consumer, we have lots of positive identities where consumers -- we know where they live -- their financial institutions know where they live, their phone numbers, identity information, their past transaction behavior as a good loyal customer. Therefore, any future transaction with that exactly same set of identities can be highly trusted. And in identity fraud, we started this three and a half years ago. People say that it's impossible to detect patterns of identity fraud. There simply isn't a pattern of social security numbers, or name and phone number that is risky versus none, which is true. But I don't think I want to justify the result on a theoretical base, but on an empirical base that, in the last three and a half years, we have successfully turned that opinion around. Before people think identity fraud is just the cost of doing business. There isn't any method that can reduce that or deal with it. And we have proved that we can actually apply, by innovation and innovation on computational techniques as well as machine learning and data modeling, basically broader analytics methods, we have increased the performance of detecting identity fraud so much that it significantly reduced the fraud cost to business.

So empirically speaking, I believe strongly that this approach works very well for identity fraud, therefore, at least as a minimum, can help solve the identity risk. In the Homeland Security area, it would be definitely good to know that someone is traveling under fake identities, under identity with suspicion. So, I don't want to venture to far beyond the identity part. I do believe -- even just to deal with the identity risk and threat, it is very valuable in the homeland security arena. I have to do more study and research. Therefore, I agree with Mary's point that further research is valuable in determining is there any other direct application of this technique.

Ms. Sotto: Mr. Turner, you have the last question before we turn to our next witness.

Mr. Turner: Thank you, Madam Chairman. I'm really curious, and my question is directed to Ms. DeRosa. I've heard a lot of panelists discuss a need for adequate controls when we're looking at the use of commercial data for various purposes. And one of the subcommittees on which I sit, I helped generate a paper looking at the use of commercial data for the reduction of false positives. And we suggested in this paper, which was then adopted by the full committee, that the controls specified in the Privacy Act be applied to information flows between the government and the commercial sector in the sense that there's some sense, particularly among the members of this committee, that there's an exemption in the Privacy Act as it's currently structured. And I'm wondering if you think that if these were applied, that those controls in the Privacy Act would be adequate, or whether you think they're insufficient? And if they're insufficient, could you speak to the Privacy Act, more generally, whether or not you think that it's perhaps, a bit anachronistic, in this day and age of more advanced modeling techniques and data mining akin to what your preceding speakers were discussing?

Ms. DeRosa: Well, I know something about the Privacy Act, sort of working knowledge. I'm not an expert. Maybe Nancy, I don't know I shouldn't speak for you. Nancy will probably talk more about that issue. So, to respond to the end of your question, I do think that, in some ways, the Privacy Act isn't really, doesn't really fit with the current uses of data, in part, because it's so focused on agency by agency, sort of a kind of stovepipe structure to -- or the philosophy of it. Which is inconsistent with a sort of focus on information sharing and the different individual agencies are -- the borders between those agencies are less significant to the general mission of counterterrorism.

About the specific types of protections in the Privacy Act, again, I'm going to defer to Nancy, who knows a lot more about those. But I think that we need to think more about in terms of databases and more about individual data than the Privacy Act does. And I think that -- so less about other kinds of broad restrictions on sharing and more about authorized, when do you have a purpose for -- you know -- does a person have a purpose for accessing a particular piece of data that is consistent with their mission? And so I guess my general comment would be more kind of thinking about individual data and less about data sets and less overall -- less agency by agency structure and more cross agency -- attention to cross agency sharing. I hope that answers your question.

Ms. Sotto: Thank you very much, Ms. DeRosa. Now we'll hear from our last witness on this panel, Nancy Libin. Ms. Libin is Staff Council at the Center for Democracy and Technology, which is a not for profit public interest organization that focuses on protecting civil liberties and democratic values in the digital age. Ms. Libin's focus at CDT is national security, government surveillance and Fourth Amendment issues. Thank you for joining us.

Ms. Libin: Well thanks for having me here today, and for giving CDT and me the opportunity to speak with you. I'm just getting over a cold, so I apologize in advance if I'm coughing through my presentation. Just as a general matter before I really begin speaking, I just want to say as a general matter, CDT believes that it's important for information technology to play a role in counterterrorism and fighting terrorism. But, it's also, I think, equally accepted certainly by CDT and indeed, it's the work of this committee that the use of information technology and commercial data, in particular, raises privacy issues. So, just setting that as sort of a framework for CDT's perspective on all of this. I want to commend the committee on its most recent report, the report on the use of commercial data to help screen out false positives in screening programs. II think the report provides an excellent policy framework for DHS to build upon.

There are a couple of issues that the report didn't address and indeed, was not intended to address, but just again, as a background, I think it's important to raise a couple of issues. The first question I think that should be asked is, when should the government conduct screening? When should it put in place a screening program? And I think it was Mr. Leo who brought up, earlier today, the Specter-Leahy Bill that addresses the issue of the use of commercial data by government and, in that piece of legislation, actually notes that -- or recommends or mandates, rather, that Congress authorize any government screening program. That is the view that CDT takes, and believes that government should authorize any screening programs, should provide rules for its operation and should determine whether it's cost effective and necessary.

Second critical question I think is, what is the government screening for? And there are other obvious problems other than the issue of false positives. With respect to the watch list, for instance, I think we need to make sure that we have adequate information to guarantee that there really are terrorists with those names that are on the watch list. We need to evaluate how we came to that conclusion that whether the methodology of determining that is reliable. So in addition to finding out whether we have enough information on the airline passenger or on the job applicant, we need to also be vigilant about the information we use to put people on the watch lists in the first instance.

Getting back to the report again, it's an excellent policy framework, and the CDT commends the committee for recommending that DHS subject itself to the provisions in the Privacy Act whenever it acquires and uses commercial data from private sector databases. Regardless of whether the agencies use in a particular instance could be deemed to fall outside of the provisions of the Act. As a general principle, and I'm sure you all know this, the Privacy Act requires the federal government to give notice to, and obtain consent from individuals before it collects and shares information about them. It requires the government to give citizens the right to see the information that the government has collected about them, and it requires, this I think gets to the data integrity mandate of the company -- requires the government to insure that the data is accurate, and relevant, and timely, and complete. But, the Privacy Act, as Mr. Turner mentioned just a moment ago, does not apply to private sector databases. There is a provision of the Privacy Act that extends its coverage to databases that are created by government contracts, but it doesn't apply to the government's use of commercial data from pre-existing databases - databases that were not created solely for the use of the government. But, again, as Mr. Turner mentioned -- and it is CDT's view that the Privacy Act, we believe, is largely outdated, and Congress certainly didn't contemplate, back in 1974, that the federal government would be acquiring data from the kinds of commercial databases that are available today. But we do believe, and I will say with a caveat because I think Mary raised a really good point about the importance of information sharing across agencies for counterterrorism purposes, and that -- putting that issue aside. In general, I think the principles on which the Privacy Act is grounded apply with equal force to the government's use of commercial data, however obtained, whether from private sector databases or otherwise, particularly in the context of national security. Just a couple of comments, if I may, on the report, which again, provides great policy framework. There are a couple of areas I thought that might be useful to clarify. The report doesn't discuss the agency's need to publish, what the Privacy Act calls a Systems of Record Notice, also called a SORN. And I think it would be useful if they also do this before they access commercial data for -- or any other -- collect data for any purpose. But, particularly in the context of using commercial data -- acquiring commercial data for screening programs. I think it would be useful if the report made clear that the agency needs to publish a SORN. Particularly when it uses commercial data for national security purposes and screening purposes. Notice is an important component of the Privacy Act. But, it doesn't solve all the problems. There are other principles in the Privacy Act that are equally important to insuring adequate privacy protection. And there's one other part of the report that I think should be -- could use some clarification. The report, I believe recommends that DHS disclose what kinds of third parties will have access to the data and whether they'll have the right to transfer the data to other affiliated or non-affiliated parities. And what I'm about to say is somewhat intentioned with what Mary -- the point that Mary raised. That's something that is worth looking into and trying to resolve. Because the notion of information sharing is intentioned with the Privacy Act principle that information that's collected for one purpose, should not be used for another purpose.

So, the part of the report that addresses the need to disclose when the information will be shared with non-affiliated or affiliated entities, I think is something CDT would recommend not happen at all. That there be no subsequent transfers of data. If it were limited to the context of counterterrorism that would be within -- I think of the Privacy Act. And that would have to be made clear - that subsequent transfers of data would be for the purpose for which they were originally collected. And that would be for national security purposes or whatever. But, that wasn't entirely clear in the report. And that was just something that could use some clarification.

This is, I think one case where merely adhering to the Privacy Act isn't entirely sufficient. There's a routine use exemption in the Privacy Act that allows such transfers of information if those transfers are consistent with routine uses that have been disclosed in the Systems Records Notice. This routine use exemption has been so broadly construed over the years as to provide at times, fortunately no limitation on the transfer of data. And thus undermine that Privacy Act principle I just mentioned, that data collected for one purpose not be used for a wholly unrelated purpose. So, I just flag that for you as something to consider.

Obviously the next task, I believe for the committee would be to determine how to answer the difficult questions of how best to implement the principles articulated through specific procedures. And CDT -- we certainly look forward to working with the committee if we can be of help to you in doing that. In filling in the details of the policy framework, the committee might turn to the Privacy Office's recent -- fairly recent guidance from privacy impact assessments. I think this was mentioned earlier today by Ms. Cooney. And the Privacy Office has really done a great job of putting together some very useful guidance.

The E-Government Act of 2002 requires agencies to conduct privacy impact assessments whenever they develop or procure new information technology or initiate a new collection of information on 10 or more people. And CDT believes these are really useful tools, both for the public and for the agency. It really gives the agency the chance to look at privacy issues at the outset. And because it requires communications between the Program Officer and the Privacy Office, it allows the concept of privacy to be built in to the infrastructure of whatever system, or technology is being instituted. CDT's a big believer in this concept of privacy by design as really being the most effective and efficient way to insure the proper privacy protections are in the system rather than having to retrofit whatever system or program you put in place. So, I commend the PIA guidance to the committee if it wants to look for ways to implement these principles. The -- two things, the E-Government Act didn't specifically require agencies to perform PIA's when they acquire commercial data from commercial databases. And the OMB guidelines allow agencies to avoid this when the use private sector databases. CDT doesn't agree with this approach. We believe the private sector entities that provide commercial data have different privacy policies and different security safeguards. And that PIA's are a useful process to determine whether there were sufficient safeguards in place, are a good opportunity to analyze those issues. DHS's Privacy Office's recent guidance on this actually suggests that it will require DHS to conduct PIA's, even when the program contemplates the use of a private sector database. And we think this is exactly the right approach. In addition, I believe there is also an opportunity for an agency to exempt itself from the requirement -- conduct a PIA when the program involves -- is in the national security context. And I would just note that the FBI, in it's own internal guidelines has nonetheless required the performance of PIA's even for programs that involve national security. And we recommend that DHS -- we would recommend DHS do the same thing. And with that, I'll just leave it at that. And answer any questions anybody might have.

Ms. Sotto: Thank you very much, Ms. Libin. I just want to note that Ari Schwartz appeared before this committee several months ago, and in part because of his testimony we are on this committee undertaking to an examination of the Privacy Act to in fact determine whether portions of it are outmoded and require revamping. John Sabo is heading that effort, so let ask you to say a few words about that please.

Mr. Sabo. Yeah, just a couple of comments. At the last meeting we announced that we were going to undertake an initiative to examine -- in effect examine the principles in the Privacy Act, safeguard and notice and so on - and their applicability in today's technology environment. And as I mentioned earlier today, if you look at Secure Flight, in our analysis of Secure Flight, one of the issues you run into is that a SORN, or a System of Records Notice for Secure Flight might reference the fact that it's riding on other systems. And those other systems may have or may not have SORN's. And those other systems might have PIA's. But, who's looking the composite system? And that's an example where the Privacy Act is not necessarily adequate. But, whether it's adequate or not, it could be that an agency in your department like DHS chooses to go beyond the Privacy Act, as an example. And look at the principles and say, how can we apply these principles across a combined system? Another area might be compliance, and is compliance, you know as required under the Privacy Act adequate to deal with technologies? So, we were going to -- undertaken enough or it hasn't started, because some of the other initiatives we have. But, I'm assuming we're going to start in January and begin looking at that. But, I think that's an important effort. Because otherwise our compliance and overall privacy management and security management aren't really possible to insure public trust, if we don't examine it in that light. So, that's just an overview of we're beginning to do under the leadership of the Framework Committee, John and Jim.

Mr. Sotto: Thank you very much, John. Joan McNabb? Did you have a question? No. Okay. David Hoffman?

Mr. Hoffman: I just wanted to thank you very much for coming here today, and you're positive comments about our paper is very welcome. And I thank you for those. I was just wondering, following up on those if it would be okay for us to ask you to submit your recommendations for either modifications or more analysis on the paper in writing?

Ms. Libin: Absolutely.

Mr. Hoffman: That would be great. And if you could do those in the context of recognizing what we announced earlier, that we are going to be taking as we have said before that paper, hopefully to another level, and taking instead of the analysis just at false positives, the overall use of commercial data. Any insight that CDT would have in that area and recommendations for the direction of that analysis would be fantastic.

Ms. Libin: That would be great. Yeah. Excellent. Thanks.

Ms. Sotto: This is unusual. This is a very confident committee. Oh, I see one. Okay.

Mr. Wright: This was already up Lisa.

Ms. Sotto: I'm sorry, my apology.

Mr. Wright: Well, Nancy you raised to very, very important questions that we started to struggle with in the screening's subcommittee up front, which is - when should the government do screening and what is government screening for? Even prior to that as we've started -- we've asked the Privacy Office to just list screening programs around the department. We started to struggle with the question of what is screening? And some of the legacy issues, I think that Jim -- look forward a bit to the immigration origins. But, could you just expand a little bit on your thoughts or what CDT is -

Ms. Libin: On screening programs, in general?

Mr. Wright: Uh-huh (affirmative).

Ms. Libin: Well, I think that one of the reasons why we feel strongly that screening programs should be congressionally authorized is to obviously provide that transparency, that opportunity for -- you know the public to be engaged considering some use of these programs. I think the other thing -- the other reason is that I think the consequences of a screening program are such that it raises obvious due process questions. And I think that was actually -- I'm just sort of remembering another issue in the report about when to use commercial data in the screening program, regardless of what the purpose of what the screening program is. Just as a general theoretical matter whether the strongest argument for the use of commercial data would be when the consequences are severe of the screening program, and when the individual who's affected by the screening program, or an adverse determination wouldn't know about that. And that that might be the strongest argument. And I -- it just reminded me of it when you asked that question. Because, I think that raises just another issue of whether there ought to be any -- that kind of secret decision making at all. And whether the lack of opportunity for redress is a problem in and of itself. And it might be worth taking a step back and looking at any screening program, and making sure that all of those due process considerations, to the extent possible are in place. And make sure that someone has the opportunity to address an adverse decision we made about that person. I think that's one of the concerns about screening programs is that the consequences can be so detrimental obviously, anything from denying someone a job, or a chance to get on airplane, to detention and deportation, that these programs really have to be thought out properly and it's proper for Congress to provide some sort of operational framework for them in the first instances.

But about specific screening programs I don't -- you know I'd be happy to talk about that as well, but as a general matter.

Ms. Sotto: Joe Alhadeff.

Mr. Alhadeff: Apparently Ramon and I live in the blind spot of the war bowls. I guess when we were looking at screening programs, and we did it ourselves, there's a natural tendency to focus on the ill effected individual who is inconvenienced or in some way subject to scrutiny that is potentially harmful to them in their daily life, or even at a less perhaps traumatic level in their travel, ability to travel, or ability to catch their plane on time. And it struck me that Jeff in his presentation talked about anonymized directories and while they don't necessarily help you prevent that false positive from occurring. They do actually limit the amount of information that is screened in the first place at a personally identifiable level. And I was just wondering, since CDT is kind of in the business of helping protect those kinds of rights, what the opinion of CDT was on doing screening in methods in which less PII is used in the first place, because we just tend to focus where there's the harmful effect as opposed to the overall impact on privacy which maybe less evident but becoming perhaps more pervasive.

Ms. Libin: Well yes I think on CDT certainly. And there are people at CDT who are involved in the Markle Foundation Task Force which has looked at these issues in more detail than I, but absolutely. I think I was just operating here just under the assumption that commercial data will be used. And taking that as a given. I think that is where CDT is. I mean I think obviously the less PII that can be used to make these determinations all the better. I think there are instances where its use is necessary, and I'm not sure if I'm really getting at your question and maybe I didn't quite fully understand your question and I apologize if that's the case. But I think to the extent that can be anonymized and still accomplish the security goals all the better.

Ms. Sotto: Thank you, Mr. Harper.

Mr. Harper: I appreciate your observations on the Privacy Act, and the difficulties where privately held collected data, and collected data is used for government decision making and I think we've done some good by suggesting the Privacy Act protections that apply in those context. But there are a variety of ways that those kinds of programs can be structured. And I'm interested if you would also apply, recommend that we suggest applying Privacy Act protections where the government never accesses the data, but rather gets a score for example, from an analysis for a more data aggregator. Should Privacy Act protections apply where government decision making is involved, or just when government has access to data.

Ms. Libin: That's a very interesting question. And I think that that really does get to the point that has been made earlier, and the Privacy Act really is out-moded and it wasn't meant to apply to the kinds of ways in which the government can act, or that are made possible by the technology that exists today. I would have to think about that more carefully, and I would like to think about that more carefully because it is a really interesting question. There's certain things obviously -- the extent to which decisions are going to be made about individuals based on information that the government is going to use, whether it's the government's directly analyzing it itself, or making a decision and acting on the use of that information. I think that some of the dangers, I'll use the word dangers but that the Privacy Act is meant to get at are still applied in that instance and one would be that there's bad data out there, and the danger that someone is going to be denied a right or a privilege or is going to be -- it's going to be the subject of an adverse determination because of bad data, still would exist in this scenario that you pause it. And I think that it would be ideal if there are ways in which to ensure that individuals had the opportunity to correct bad data about them that is going to be used to make decisions about them. I'm speaking very theoretically here and would have to think that through more carefully, but I do think the principles still apply. If it's just a score I'm not sure how that would work exactly. But there is still that danger out there.

Ms. Sotto: Mr. Wright.

Mr. Wright: Somewhat of an observation, I'd just appreciate your thoughts. A lot of the discussion concerning the Privacy Act and its implication here and the sensitivities we should have about the Privacy Act. My understanding and correct me if I'm wrong the Privacy Act relates to protections of U.S. citizens and hopefully in evaluating terrorists to the United States, the vast majority of those will not be U.S. citizens, have you given any thought to whether in developing processes here that perhaps we should give some consideration to two standards, one for U.S. citizens and one for non-U.S. citizens.

Ms. Libin: Well you're right, that I think it's in U.S. persons generally are afforded greater protection than non-U.S. persons. But I think that is the way -- I mean I do that that will continue to be the case. And I don't know if Mary, this is something you've looked at, in the context of U.S. persons. I know you've done some -- I don't mean to kick this over to you.

Ms. DeRosa: I want to make sure I understand the question because I think on the one hand if we're talking about the Privacy Act, I think what you've raised is another example of where when you just say apply the controls of the Privacy Act, you're not really doing enough, because the Privacy Act isn't going to solve that problem. Generally I think there's a lot of -- I have to be careful because this is sort of sensitive issue. The issue of information sharing, different rules for U.S. persons, and non-U.S. persons and how information is shared and who can access it I think is one of the issues that we have been looking at. And the Markle Foundation Task Force, because it tends to be outdated in a way. I mean most of the info is that people looking into counter terrorism need -- really can't break down that way easily. So I think it's another area where you need to be able to think of controls, not just in the is it U.S. person, or not U.S. person, but something more in nuance to say that you can really control, you can control the use of private data without having to do an inquiry about whether it's a U.S. person or not. And what that -- that's one area where an inquiry about, is there an authorized purpose. Is when somebody is accessing data, do they have a reason for accessing the data that is related to their mission and a legitimate counter terrorism mission before somebody can access the data, that's the kind of control that really doesn't look at whether it's a U.S. person or non-U.S. person, but looks at the mission of the person getting it and whether there's a reason for it. So I don't know if that was what you were getting at or not, sort of the general U.S. person issue, then the Privacy Act part of it, which is I mean, it's another place where if you just looked at the Privacy Act you wouldn't be really doing enough I think in terms of controls.

Mr. Wright: I think to some extent you've answered my question. And obviously I mean we're going to be hearing this afternoon from representatives of the EU and what have you, where we have to provide some kind of guarantee of how data will be used if we expect to really get that data being shared with us. So I appreciate your response.

Ms. Sotto: I want to thank our panel, your comments were extremely incisive and thoughtful. And have given us a lot of food for thought. And speaking of food, we are going to close this session for the next hour for administrative activities of the committee, we will reconvene here at 1:30 for the afternoon session. Thank you very much.